Ежегодно увеличивается число обманутых владельцев банковских карт. Оружием мошенников стал телефон. Как обезопасить себя и сохранить свои деньги?

По данным РБК за 2019 год почти каждый десятый россиянин (около 9%) терял значительную для себя сумму денег из-за телефонного мошенничества, а каждый третий (33%) признался, что он или его близкие сталкивались с таким мошенничеством. Только 4% опрошенных обращались в правоохранительные органы.

Также по данным за 2018 год объем несанкционированных операций по картам вырос на 44% и составил 1,4 млрд рублей. В законе «О национальной платёжной системе» говорится, что если деньги с карты списаны без согласия клиента, то банк должен вернуть похищенную сумму. Однако таких случаев ещё не было. Банки не возвращают средства, потому что не могут различить действия клиентов и мошенничество: для этого суд должен установить виновных, а полиция не в состоянии их найти.

Знайте способы обмана!

Звонок из банка. Сейчас этот способ самый частый. В основном обзванивают клиентов крупных банков — в них обслуживается очень много людей. Из 50–100 звонков из таких «колл-центров» хотя бы один срабатывает. Клиенту звонят с использованием программ для подмены номера либо с номера, который раньше действительно принадлежал банку. Они представляются сотрудниками финансовой организации и выманивают пароли или коды для входа в личный кабинет или подтверждения перевода денег.

Звонок от родственника. Звонят с незнакомого номера. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции. Причина — ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и даже убийство. Мошенник просит перевести деньги на определенную карту — по легенде это карта друга или «помощника».

Звонок–грабитель. Человек поднимает трубку. Его приветствуют фанфары и довольный голос. Разговор тянется долго, а после выясняется, что он был платным. Есть и другая вариация такого звонка. Мошенники делают короткий звонок, чтобы он отразился на экране телефона как пропущенный. Когда человек перезванивает, со счета списывается фиксированная сумма.

Подозрительные смски. На телефон приходит сообщение от банка или оператора связи. В нем — просьба отправить определенный код или перейти по ссылке. Часто мошенники регистрируют адреса, похожие на названия известных организаций. Разница будет в одной букве — это получается заметить не сразу.

Как действуют мошенники?

Чаще всего те, кто снимает деньги у доверчивых граждан, — не один и не два человека. В «теневом» интернете есть много площадок, предлагающих продажу информации. Среди баз данных есть и банковские. Другими словами, весь ваш профиль в банке мгновенно доступен любому человеку, способному немного заплатить. Можно считать это нарушением Федерального закона №152-ФЗ. Фактически доказать это нарушение маловероятно.

Подделка номеров тоже теневая услуга. Имея доступ к системе небольшого мобильного оператора, можно подменить номер. В итоге преступник звонит со своего номера, а у абонента высвечивается любой другой, в том числе телефон банка. Как правило такие звонки могут предлагать зарубежные компании.

За день маленькая группа из нескольких человек вполне может зарабатывать несколько миллионов рублей.

Признаки мошенничества!

1. При долгом общении собеседник начинает нервничать. Если вы все же взяли трубку, то не ведитесь на рассказы мошенника о тестированиях новых систем или невозможности видеть ваши операции по карте. Так он пытается вытянуть ваши данные. Можно потянуть время и заставить злоумышленника нервничать — сказать, что ищете карту и «висеть» на телефоне минут 10-15. Или завершите разговор фразой «да, это я снимал деньги, все в порядке!». Если преступник понимает, что жертва что-то заподозрила, он просто прекратит разговор и продолжит обзванивать других. Не давайте повода усыпить свою бдительность.

Пример из жизни:

«Где-то полтора года назад я продавал бенгальских котят. Позвонила женщина — представилась руководителем какой-то компании. Якобы она решила купить котенка для своей племянницы, сама живет не в моем городе, поэтому сделку надо было провести с переводом денег.

Очень убедительно рассказала о себе, компании. Например, что котенка заберут их курьеры — «они как раз проезжают N, заедут, заберут и отдадут вторую часть денег». Задавала правильные вопросы о котятах.

Когда сошлись на цене, предложила перевести мне половину денег на карту. И сказала, что со мной свяжется человек из их финотдела. Затем перезванивает молодой человек. Представляется то ли юристом, то ли экономистом из их компании. Объясняет, что для перевода денег ему нужен номер карты, номер счета, дата, фио и код с обратной стороны карты. Такие условия необходимы, потому что «деньги переводят со счета компании, поэтому физлицо должно предоставить все эти данные, чтобы всё легально провести через бухгалтерию».

2. Смс «от банка» перешло в новую переписку. В таком сообщении может быть ссылка «для смены тарифа» или «для подтверждения зачисления средств». В таких сообщениях можно заметить ошибки в словах. Могут быть ошибки и в «имени» отправителя. Если нашли, то не сомневайтесь — это мошенники. Не переходите по ссылке, а сообщение удалите.

3. Собеседник спрашивает данные карты или смс-код. Смс-код приравнивается к паролю и по сути является простой электронной подписью.

Сотрудники банка никогда его не спросят, а номер карты они и так знают. Кроме того, подозрительный собеседник начнет придумывать новые способы получить ваши данные. Если в процессе разговора вам приходят «смс от банка» не сообщайте информацию из них и не переходите по ссылкам.

Пример из жизни:

«— Здравствуйте, ВВ! Вас беспокоит служба безопасности «Хорошегобанка». Меня зовут Усачев Дмитрий Сергеевич, я младший специалист. Мы тут зафиксировали подозрительную активность по вашей карте. Несколько минут назад пытались перевести 3 624 рубля. Это вы были?

— Да, это я снимала деньги.

— Хорошо, тогда скажите, сколько на ваше имя карт оформлено? Какая последняя операция была по ним — перевод, снятие, оплата?

— Это ж вы и сами можете посмотреть.

— У нас новая система безопасности, и этого всего не видно.

— Тогда мне тоже этого не видно.

— То есть, вы отказываетесь от проведения проверки? Подтвердите свой отказ устно в полной форме.

— До свидания!».

Как защитить свои деньги?

По данным опроса «Лаборатории Касперского», каждый пятый россиянин (21%) никак не защищает свой телефон от подозрительных звонков. Половина респондентов (51%) ответили, что не берут трубку, если видят на экране неизвестный номер. Еще 17% россиян используют специализированное ПО для защиты от спама и мошенничества, а 37% — встроенные возможности телефона, например черные списки.

Простые способы обезопасить себя и свои деньги:

1. Не принимайте звонки со скрытых или неизвестных номеров. Можно установить на телефон приложение, которое ищет владельца номера в интернете. Например, сервис Яндекса помогает избежать подозрительных звонков и спама. Нежелательные номера заносите в «чёрный список». Если вы поменяли номер своего телефона, предупредите об этом родственников и друзей.

2. Не сообщайте никому данные своей карты. Не сообщайте коды из смсок. Если забыли карточку в общественном месте — заблокируйте.

3. Не принимайте звонки с подозрительных номеров. Не перезванивайте по ним. Ни спрашивайте у них телефон банка, по которому могут что-либо подтвердить, ищите его на своей банковской карте.

4. Держите связь с родственниками и друзьями. Если вам звонят с просьбами о помощи, сбросьте звонок. Перезвоните «жертве».

5. Внимательно читайте сообщения из банка. Мошенники используют имена отправителей, похожие на названия банков, и допускают ошибки в тексте.

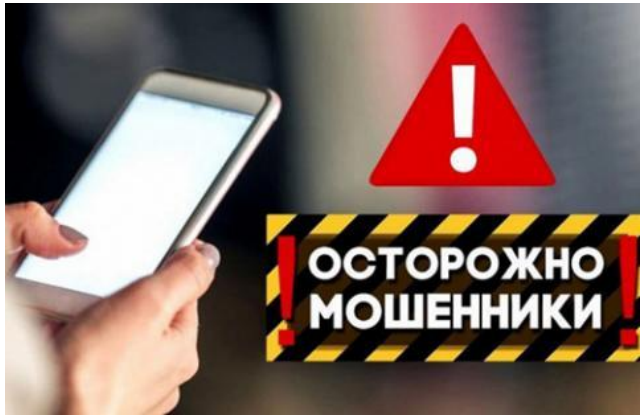
6. Не указывайте настоящий номер телефона и не расплачиваться основной картой на малоизвестных сайтах.

7. Не паникуйте, если вам пишут о блокировке счета. Позвоните в банк по номеру на сайте или на карте.

Прокуратура Республики Саха (Якутия)
677000, г. Якутск, пр. Ленина, 48,
http://https://epp.genproc.gov.ru/web/proc_14

Прокуратура Республики Саха (Якутия)

Телефонное мошенничество. Как распознать и защититься?



Якутск, 2020 год