Финансовое мошенничество.
Защити себя и свою семью

В современном мире финансовых услуг становится все больше, они усложняются, мошенники постоянно развивают технологии и «способы отъема денег у населения». Поэтому вопросы личной финансовой безопасности граждан имеют жизненно важное значение.

Стать жертвой преступников может каждый, и неважно, использует он банковскую карту или предпочитает рассчитываться наличными. Мошенники умеют выманивать деньги онлайн, с помощью звонков и СМС, в социальных сетях и офисах. Как они это делают?

Мошенничество с банковскими картами

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV. Они могут установить скиммер на банкомат (специальное устройство, которое накладывают на приемник карты в банкомате) и видеокамеру над клавиатурой.

Номер CVC или CVV - три цифры, расположенные на поле для подписи владельца карты или рядом с ним.

Достаточно один раз воспользоваться таким банкоматом и не прикрыть рукой клавиатуру в момент набора ПИН-кода - и ваши деньги могут снять, перевести на несколько счетов и обналичить. Украсть данные вашей карты могут даже в кафе или магазине. Злоумышленником может оказаться продавец, который получит доступ к вашей карте хотя бы на пять секунд. Сфотографировав вашу карту, он сможет воспользоваться ей для расчетов в интернете.

Как не попасться:

Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.

Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.

Подключите мобильный банк и СМС-уведомления.

Если совершаете покупки через интернет, никому не сообщайте секретный код для подтверждения операций, который приходит вам по СМС.

Старайтесь никогда не терять из виду вашу карту.

Меня обокрали. Что делать?

Позвоните в банк (номер всегда есть на обороте карты или на главной странице сайта банка), сообщите о мошеннической операции и заблокируйте карту.

Запросите выписку по счету и напишите заявление о несогласии с операцией.

Обратитесь с заявлением в отдел полиции по месту жительства.

Кибермошенничество

Допустим, вы всегда снимаете деньги только в кассе банка, а картой и вовсе не рассчитываетесь. Вы чувствуете себя в безопасности. Вдруг вам приходит СМС или письмо якобы от банка со ссылкой, просьбой перезвонить по неизвестному номеру или с уведомлением о неожиданном крупном выигрыше. Или звонят от имени банка и просят сообщить личные данные, ПИН-код от карты или номер СМС-подтверждения. Или пишут в социальных сетях от имени родственников или друзей, которые внезапно попали в беду (угодили в полицию, сбила машина, украли сумку) и просят перевести энную сумму денег на неизвестный счет. В 99,9% случаев вы имеете дело с мошенниками. За ссылками, скорее всего, таятся вирусы, на другом конце провода - специалисты по обману, которые всеми правдами и неправдами хотят выманить необходимые им данные, а по ту сторону экрана - злоумышленники, которые играют на ваших желаниях, чувствах и заботе о близких.

Как не попасться:

Не переходите по неизвестным ссылкам, не перезванивайте по сомнительным номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках.

Если вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть, не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС - не от вашего банка, а звонил вам злоумышленник. Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.

Если вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас код, чтобы списать с вашего счета деньги или подписать вас на ненужный платный сервис.

Никому не сообщайте персональные данные, а уж тем более пароли и коды. Сотрудникам банка они не нужны, а мошенникам откроют доступ к вашим деньгам.

Не храните данные карт на компьютере или в смартфоне.

Проверяйте информацию. Если вам говорят, будто вы что-то выиграли или с вашей карты случайно списали деньги и нужно назвать свои данные, чтобы остановить операцию, закончите разговор и перезвоните в банк по номеру телефона, указанному на обратной стороне вашей карты.

Если вам сообщают, что у родственников или друзей неприятности, постарайтесь связаться с ними напрямую.

Установите на компьютер антивирус - и себе, и родственникам.

Объясните пожилым родственникам и подросткам эти простые правила.

Мошеннические организации

Самая известная мошенническая организация в России - МММ. Она работала по принципу финансовой пирамиды: обещала огромные проценты по вкладам, гарантировала доходность и выплачивала средства за счет денег, внесенных другими вкладчиками. Верхушка этой пирамиды действительно могла заработать, а те, кто стоял на ступенях ниже, теряли свои деньги. Но сейчас ситуация изменилась, организаторы финансовых пирамид - просто мошенники, которые собирают с людей деньги и пропадают. Неважно, вверху вы пирамиды или внизу, на финансовых пирамидах заработать нельзя: если вы вложите деньги, вы непременно их потеряете.

Сейчас финансовые пирамиды начинают маскироваться под микрофинансовые организации, работающие по принципу сетевого маркетинга, инвестиционные и управляющие предприятия, онлайн-казино. Они заявляют о высоких процентах по вкладам и отсутствии рисков, гарантируют доход (что запрещено на рынке ценных бумаг), обещают помощь людям с плохой кредитной историей. А еще просят внести деньги сразу (желательно наличными) и привести друга (иногда за какой-то бонус), чтобы масштабы пирамиды увеличивались и их (а не ваша) прибыль росла.

Как уберечься от обмана:

Финансовая организация должна иметь лицензию или быть в реестре Банка России. Сверьтесь со справочником участников финансового рынка.

Проверьте компанию в Едином государственном реестре юридических лиц ФНС России.

Запросите образцы договоров, копии документов. Если есть возможность, проконсультируйтесь с юристом.

Мошенничество на финансовых рынках

Еще один тип мошенников - псевдопрофессиональные участники финансового рынка, которые активно рекламируют свои услуги по организации торговли на рынке Форекс.

Наверняка вы слышали истории, как простые люди «с улицы» заработали состояние, покупая и продавая валюту на рынке Форекс. Звучит заманчиво, но не спешите рисковать. Физическое лицо с небольшим стартовым капиталом не имеет доступа на реальный рынок Форекс, где продают и покупают валюту в основном крупные банки. Чтобы обычному человеку выйти на Форекс, нужно заключить договор с посредником, форекс-дилером, и торговать через него.

Торговля на рынке Форекс сама по себе большой риск, гарантий нет, больше шансов потерять все, чем сорвать куш. Но опасность кроется и в посредниках: можно нарваться на мошенников, которые просто не вернут вам деньги. Вероятен такой вариант: вам предлагают удивительно низкие комиссии, различные бонусы (сумма на вашем счете, допустим, удваивается). Вы даже можете заключить с дилером договор через интернет с помощью электронного документооборота и вроде бы выиграть целый миллион! Но прибыль вы не получите и вложения потеряете.

Если вы стали жертвой мошенничества на финансовых рынках

Соберите все документы, которые у вас есть: договоры, заключенные с посредником-мошенником, чеки на перевод денег, сделайте скриншоты с сайта - и отправляйтесь в полицию писать заявление.

Сообщите в Банк России, все жалобы рассматриваются.