

Как уберечь себя и близких от финансового мошенничества

Списание денег со счета без ведома владельца, кража паролей и ПИН-кодов, легкий заработок в интернете и вклады под невероятные проценты, онлайн-казино — все это виды финансового мошенничества. Преступники будут спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или государственные организации, чтобы выманить деньги. Как распознать мошенника и что делать, если вас все-таки удалось обмануть?

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.

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;

МОСКОВСКИЙ ЦЕНТРАЛЬНЫЙ
 3042 03. 2022

- 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.

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 (утодили в полицию, сбила машина, украли сумку) и просят перевести эту 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 по кредитным организациям и 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.