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.
- 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

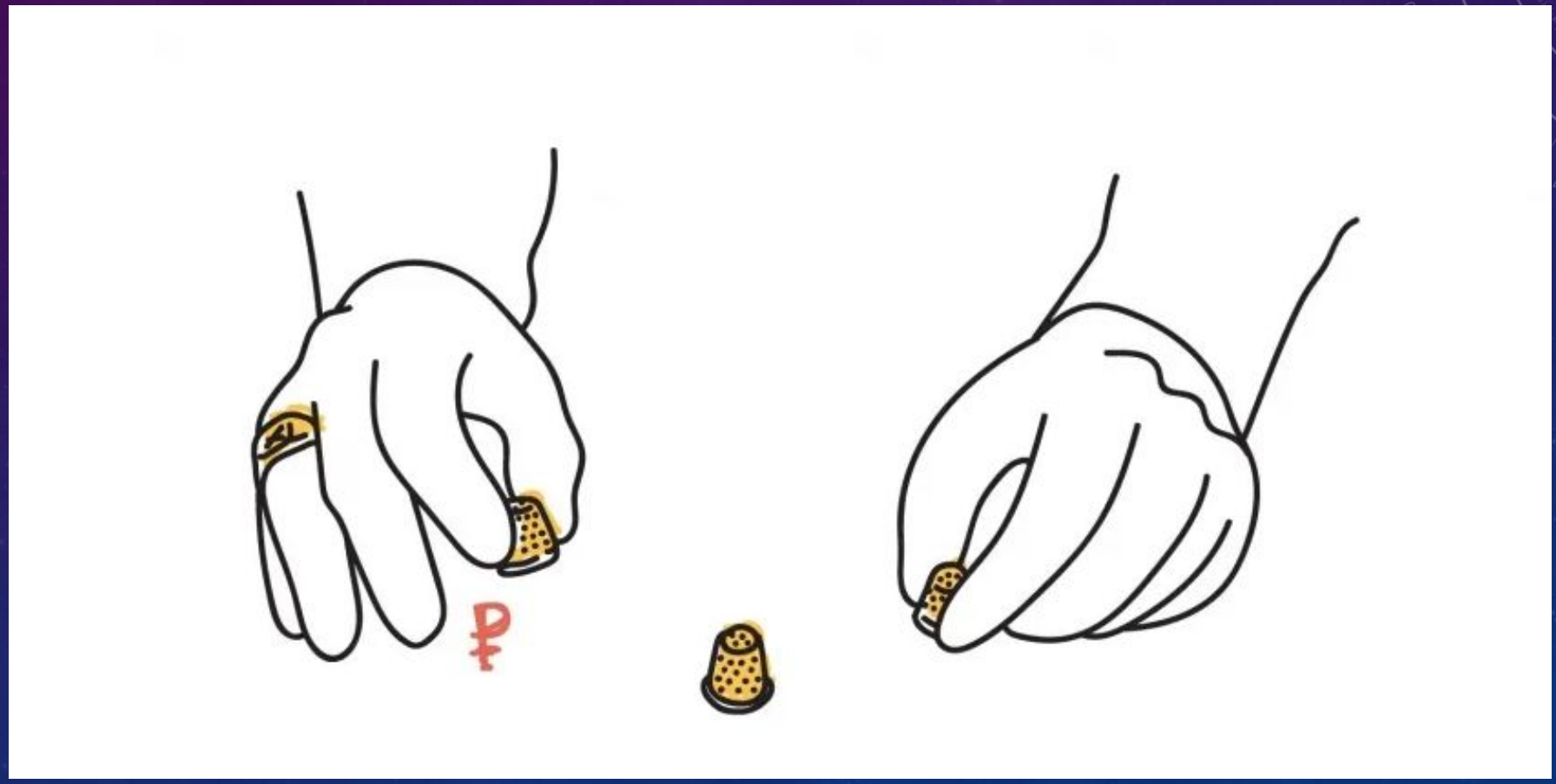
- Допустим, вы всегда снимаете деньги только в кассе банка, а картой и вовсе не рассчитываетесь. Вы чувствуете себя в безопасности. Вдруг вам приходит СМС или письмо якобы от банка со ссылкой, просьбой перезвонить по неизвестному номеру или с уведомлением о неожиданном крупном выигрыше. Или звонят от 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 (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.

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.