Как уберечь себя и близких от финансового мошенничества

Финансовые мошенники очень изобретательны. Но главное, что помогает им «зарабатывать», — излишняя доверчивость людей. О чем нужно помнить, чтобы не стать жертвой аферистов? Разбираемся, как распознать мошенников и что делать, если вас все-таки обманули.

Как происходит мошенничество с банковскими картами и как его избежать?

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV (три цифры, расположенные на поле для подписи владельца карты или рядом с ним). 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 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.

Чтобы не попасться на уловки мошенников, 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 в СМС. Старайтесь никогда не терять из виду вашу карту.

Как действуют кибермошенники?

Они могут назваться кем угодно и придумать самые разные легенды. Часто представляются сотрудниками банков, страховых и инвестиционных компаний; полиции, налоговой или ГИБДД, социальной службы, медицинских, благотворительных или других организаций. На сайтах объявлений они выступают как продавцы или покупатели. Бывают случаи, когда они выходят на вас как будущие работодатели или коллеги. Иногда мошенники используют даже ботов – роботизированных виртуальных помощников.

Но кем бы они ни прикидывались, их можно отличить по нескольким признакам. Они выходят на вас сами и речь всегда идет о деньгах. Стараются вызвать сильные эмоции: страх, радость или гнев: так они сбивают вас с толку, чтобы не дать вам мыслить рационально. Вас торопят и запутывают, не давая шанса обдумать ситуацию и распознать обман. Они попытаются выманить у вас данные карт, например, с помощью ссылок на вирусные или фишинговые сайты, где нужно ввести банковские реквизиты. Или постараются выведать логины и пароли от онлайн- или мобильного банка, Портала госуслуг или других личных кабинетов, через которые можно добраться до ваших счетов.

Нередко преступников интересуют ваши персональные данные, паспорт, СНИЛС и ИНН. Зная эту информацию, они могут, например, попытаться взять кредит на ваше имя. Или используют эти данные в других схемах социальной инженерии.

Как не стать жертвой кибермошенников?

Не торопитесь и всегда 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 родственники или друзья попали в беду, постарайтесь связаться с ними напрямую. Никому не сообщайте и не вводите на сомнительных сайтах личные данные (из паспорта и других документов), полные реквизиты карты, пароли и коды из уведомлений от банка. Не вводите их на подозрительных сайтах.

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.

Не храните данные карт на компьютере или в смартфоне. Установите антивирус на компьютер и все свои гаджеты. Расскажите родственникам и знакомым об этих простых правилах.

Что делать, если человек все-таки стал жертвой мошенников?

Немедленно обратитесь в банк по телефону (номер горячей линии банка указан на обратной стороне карты) или через официальное мобильное приложение и заблокируйте карту. Запросите выписку по счету и напишите заявление о несогласии с операцией. Обратитесь в полицию. Чем быстрее вы это сделаете, тем выше вероятность того, что преступников найдут и привлекут к ответственности.

Текст статьи подготовлен на основе материалов информационно-просветительского ресурса Fincult.info (https://fincult.info/)