

Банкиры зафиксировали активизацию деятельности мошенников, которые используют психологические методы давления на граждан с целью изъятия их средств с платежных карт.

Чаще всего мошенники, вводя граждан в заблуждение, пытаются выманить данные карт или заставить осуществить перевод средств на чужой счет.

Психическая атака

Банкиры столкнулись с активизацией одного из видов мошенничества с платежными картами и денежными переводами. Речь идет о несанкционированном доступе к деньгам посредством оказания психологического давления на их владельца, рассказали в Украинской межбанковской ассоциации членов платежных систем ЕМА.

Вариантов такого мошенничества (банкиры называют его социальной инженерией) несколько. Оно строится вокруг значимых для людей тем, например, событий, связанных с военными действиями на востоке, или с личными переживаниями. Чаще всего держателей платежных карт вводят в заблуждение при совершении операции перевода средств. «Человек собирает деньги для помощи и лечения раненного в АТО родственника. Ему звонит очередной «меценат» и сообщает, что он перечислил деньги, но они якобы заблокированы, так как перевод осуществлен от юрлица. Для «разблокировки» он предлагает держателю карты ввести в банкомате названный ему номер, который должен разблокировать эти деньги и они должны упасть ему на карту. Однако через банкомат невозможно зачислить деньги с чужой карты на свою, только наоборот. Поэтому человек фактически сам (добровольно. – Ред.) переводит деньги со своей карты на карту мошенника», – рассказывает ведущий специалист службы защиты

платежных систем Фидобанка Игорь Попов.

«Или человек вывешивает объявление о продаже товара на сайте интернет-аукциона. Ему звонит покупатель, который готов перечислить деньги на карточку. Но при этом просит дать все данные карты, а не только номер, и человек по незнанию дает их. Или звонит и говорит, что продиктует какой-то номер для осуществления перевода», – перечисляет все примеры Игорь Попов.

Не обходят стороной мошенники и сбор данных с платежных карт. «К нам приходили разъяренные клиенты, которые заявляли, что им звонили сотрудники банка и говорили о каком-то сбое в системе или о поломке сервера. И просили дать всю информацию о картах для восстановления данных: номер, пин-код, CVV, – рассказывает заместитель председателя правления одного из банков. – Это однозначно мошенничество, потому что сотруднику банка эти данные не нужны никогда».

Участились случаи мошенничества, связанные с социальными выплатами. «Беженцы с востока получают информацию, что им хотят начислить пособие. Но для этого просто надо предоставить все данные карты. И люди дают пин-коды, а потом теряют все средства, которые у них были», – говорит руководитель Форума безопасности расчетов и операций с платежными инструментами ЕМА Олеся Данильченко.

Мошенники набирают обороты

Социальное мошенничество популяризируется, поскольку у преступников сократились иные возможности для выгодного обмана граждан. «Все виды мошенничества, связанные с денежными расчетами, с начала года идут на спад. Это касается банкоматного мошенничества, преступлений в интернете, эквайринговой сети, системах дистанционного банковского обслуживания и кредитного мошенничества. Это происходит из-за того, что были введены лимиты на снятие наличных и безналичные переводы, а также уменьшились объемы кредитования, – поясняет Олеся Данильченко. – Поэтому преступники начинают придумывать новые виды мошенничества».

Точное количество таких преступлений неизвестно, так как граждане далеко не всегда обращаются в правоохранительные органы в таких случаях. Однако оно уже довольно

велико. «Каждый день к нам поступает порядка 20 жалоб от людей на подобное мошенничество, – рассказывает начальник организационно-аналитического отдела УБК МВД Леонид Тимченко. – В прошлом году в Херсонской области была задержана группа мошенников, которая нанесла ущерб гражданам по всей Украине на 400 тыс. грн. На прошлой неделе была задержана еще одна группа, которая совершила более 500 преступлений в отношении пользователей интернет-аукционов».

В ЕМА рассказали, что после исследования, проведенного в одном из банков, оказалось, что 12% платежей, которые осуществляются через банкоматы, проходят на счета мошенников. Примечательно, что эти мошеннические операции не являются убытком банков, так как по сути представляют собой обычный перевод между двумя счетами. Поэтому общий размер ущерба, нанесенного гражданами такими мошенниками, неизвестен.

Возможности отслеживания

Для защиты от такого вида мошенничества банкиры советуют гражданам не давать никому данные платежных карт, не следовать советам якобы сотрудников банков, которые звонят с невидимых или неизвестных номеров, а также не вводить в банкоматах непонятные комбинации цифр. В таких случаях стоит сразу же оповестить банк и правоохранительные органы о попытке мошенничества.

Банкиры стараются бороться с такими преступниками. Хотя фактически это даже не является киберпреступлением, а относится к обману и введению в заблуждение. «Фактически человек сам передает деньги мошеннику. Но мы расследуем такие случаи. Смотрим, на какую карту падают деньги, какие номера телефонов используются. А если мошенник пользуется банкоматом, то мы получаем его фото, – рассказывает заместитель руководителя направления «Общий маркетинг и реклама» ПриватБанка Олег Серга. – Потом мы передаем эту информацию в МВД. Несколько банкиров, которые занимались таким в Киеве, Сумах, Днепродзержинске и Луганске, уже сидят в тюрьме».

Теоретически эти средства можно попробовать вернуть. «Если деньги ушли со счета человека на какой-то счет в другом банке, но они еще не сняты, то можно предупредить этот банк о случившемся преступлении», – говорит Игорь Попов.