Мошенничество в сфере финансовых услуг

Мошенничество в сфере финансовых услуг с каждым годом набирает обороты и списывает со счетов граждан значительные суммы.

В 2022 году в России зафиксировано 129 тысяч случаев использования платежных карт без согласия их владельцев в банкомате или терминале на общую сумму 1,6 млрд руб.

В прошедшем году клиенты банков — физические лица сообщили о 516 тыс. операций без их согласия, совершенных при оплате товаров и услуг в Интернете (CNP-транзакции), 48,7% из которых — результат применения к ним приемов и методов социальной инженерии (мошенники вводят людей в состояние стресса и поскольку человеку называют его персональные данные, он начинает верить звонящему и готов исполнять указания). Сумма хищений составила 2,55 млрд. рублей.

К ранее используемым сценариям звонков злоумышленников, а именно звонков от якобы «специалистов службы безопасности банка», «правоохранительных органов» и «Центрального банка», добавились сценарии, связанные с частичной мобилизацией.

В нашей области звонки или сообщения от мошенников поступают чуть ли не каждому второму жителю. Наивно предполагать, что жертвами этих злоумышленников становятся только пожилые люди, это далеко не так. Как поясняют сотрудники правоохранительных органов, на уловку криминальных элементов может попасть абсолютно каждый.

Рассмотрим самые популярные мошеннические схемы, зафиксированные в нашем регионе.

Звонит телефон. Собеседник на другом конце провода представляется сотрудником правоохранительных органов, как правило, высокого звания и сразу заявляет, что сын/дочь/муж попал в дорожно-транспортное происшествие или сбил человека. Конкретики никакой. Чаще всего в процессе разговора жертва сама называет имя своего родственника. Затем поддается панике, что играет на руку мошенникам. Если на этом этапе человека удалось ввести в заблуждение и тот

начинает верить, то ему предлагают заплатить некую сумму денег, если такой суммы нет, то следует вопрос: «А сколько у вас есть?», в итоге мошенник соглашается на предложенные деньги. А дальше дело техники и индивидуального подхода к собеседнику.

Самый привлекательный для мошенников объект — данные банковской карты, благодаря которой можно лишиться сразу всей суммы на счету. Например, поступает звонок или СМС от якобы сотрудника банка, что у вас заблокирована карта. При этом выливают поток абсолютно ненужной информации, не давая опомниться, и в процессе разговора вы сами диктуете необходимые данные или совершаете нужные для мошенников манипуляции, находясь у банкомата.

Мошенники умудряются одурачить даже тех, кто продаёт свои вещи на специальных сайтах. К примеру, вы разместили в Интернете объявление о продаже старого телевизора. Злоумышленники звонят и говорят, что готовы купить технику. Сейчас подъехать не могут, но хотят заплатить. Они просят продиктовать реквизиты вашей карты, чтобы перевести деньги. Ни в коем случае не верьте и не называйте данные.

Незнакомец представляется социальным работником и сообщает о надбавке к пенсии, перерасчете квартплаты, премии ветеранам, срочном обмене денег на дому якобы «только для пенсионеров». Каким бы любезным или участливым не был этот человек — это мошенник.

Еще одна популярная тема среди обманщиков — сайты купли-продажи. Рассмотрим схему с покупкой автомобиля. Вы находите нужное вам объявление, где автомобиль вашей мечты выставлен по бросовой цене, ничего не заподозрив, набираете номер телефона. Вам рассказывают, что машину нужно продать срочно, поэтому цена невысокая и уже очень много желающих купить этот автомобиль. Затем предлагают подтвердить серьезность ваших намерений и совершить предоплату, диктуют номер телефона, куда перевести деньги. После перевода номер телефона уже не доступен. Все вышеперечисленные случаи — лишь примеры, в реальности события развиваются стремительно, мошенники действуют изощрённее, но цель у них одна — узнать нужные данные вашей карты или сыграть на эмоциях.

Помимо мобильных телефонов, злоумышленники могут использовать взломанные аккаунты ваших друзей и знакомых в социальных сетях. Цель одна — перевод денежных средств.

Чтобы сохранить при себе свои деньги, нужно соблюдать простые правила:

1. Обязательно подключите банковскую систему смс-оповещения обо всех операциях и/или систему push-уведомлений через онлайн-приложение вашего банка. В случае любой информации об операции (даже самой мелкой), которую вы не совершали, сообщите в службу поддержки банка по телефону, указанному на карте.

2. Проверяйте состояние счета после любых операций с картой. Если остаток на счёте не совпадает с вашими ожиданиями, внимательно просмотрите все последние смс-сообщения от банка о ваших транзакциях.

3. При покупке или продаже любого товара или услуги НИКОМУ не называйте конфиденциальные данные своей банковской карты: не сообщайте PIN-код и CVV2-код карты (цифры с обратной стороны карты), а также срок её действия и персональные данные владельца.

4. Не выполняйте указаний незнакомых лиц при действиях с банковской картой. 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 вашей карте.

5. Проведите разъяснительную беседу с пожилыми родственниками, доступно объясните им, что нельзя рассказывать о себе конфиденциальную информацию посторонним и неизвестным людям.

Что делать, если мошенники всё же украли деньги с карты?

1. Позвоните в банк по номеру телефона, указанному на карте, сообщите о мошеннической операции и заблокируйте карту.

2. Запросите выписку по счёту и напишите заявление о несогласии с операцией.

3. Обратитесь с заявлением в отдел полиции по месту жительства.

М.А. Нашкеева,

заместитель мэра по экономике и сельскому хозяйству.