

19 → Анна Зайцева, аналитик УК «Финам Менеджмент», отмечает, что в розничном сегменте на сегодняшний день мошенники оперируют широким набором инструментов и весьма высокотехнологичных решений в сфере процессинга. «Одним из наиболее распространенных видов противоправных действий остается кардинг — несанкционированные операции с банковскими картами», — заключает она.

Лариса Магерио, управляющий филиалом «Петровский» банка «Открытие», говорит, что большое количество мошенничеств происходит с использованием пластиковых карт. «Банковская карта с микропроцессором (чипом) является более защищенной, чем карта только с магнитной полосой. Данные, хранящиеся на встроенном чипе, скопировать технически намного сложнее, практически невозможно, поэтому банк „Открытие“ выпускает только чиповые карты, в том числе безымянные моментального выпуска. Если владелец чиповой карты забыл ее в магазине или потерял, риск того, что к моменту обнаружения пропажи картой воспользуются третьи лица, снижен до минимума. Но даже такая карта не сможет защитить от мошенничества при совершении операций в интернете, поэтому для этих целей лучше завести виртуальную карту», — предостерегает она.

ОТ ФАЛЬШИВЫХ БАНКОМАТОВ ДО ФИНАНСОВЫХ ПИРАМИД

Эксперты также приводят в пример и другие виды обмана.

В частности, Владимир Климов, директор регионального центра банка «Хоум Кредит» в Санкт-Петербурге, говорит, что мошенники могут позвонить или прислать письмо с запросом личных данных клиента банка под придуманным предлогом. «Отличить письмо от банка от письма, составленного мошенниками, очень просто — банк никогда не запрашивает данные клиента онлайн. Другими словами, вся та информация, которая необходима для получения кредита (номер паспорта, адрес прописки, место работы), запрашивается банком только в момент оформления кредита лично у клиента, — говорит он. — Однако банки могут на своем сайте просить заполнить онлайн-заявку на кредит, на нашем сайте, например, мы запрашиваем ФИО, дату рождения, регион проживания, прописку, размер ежемесячного дохода и контактные данные. Это так называемый прескоринг, когда на основе первичных данных кредитный специалист рассчитывает для клиента возможное предложение. Однако для процедуры оформления кредита клиент все равно должен будет прийти в офис и предоставить необходимые документы».

Господин Климов солидарен с другими экспертами в том, что одним из наиболее часто встречающихся видов финансовых преступлений является мошенничество с банковскими картами. По его словам, в его банке работает мониторинг сомнительных транзакций. «Если операция по карте вызывает какие-либо сомнения в том, что она осуществлена клиентом, банк незамедлительно уведомляет об этом клиента. Чаще всего имеет место так называемый family fraud — когда картой воспользовался кто-то из родственников или знакомых, а клиент просто недостаточно надежно сохранял карту или свои данные. Также распространенным ви-



НЕСМОТЯ НА ТО, ЧТО БАНКИ ПОСТОЯННО СООБЩАЮТ КЛИЕНТАМ ПРОПИСНЫЕ ИСТИНЫ О СПОСОБАХ ЗАЩИТЫ ОТ МОШЕННИКОВ, ГРАЖДАНЕ ПРОДОЛЖАЮТ ДОПУСКАТЬ ПРОМАХИ

дом мошенничества является скимминг, то есть считывание данных с магнитной полосы для последующего изготовления поддельных карт. Для минимизации риска компрометации данных с магнитной полосы карты желательно использовать банкоматы, находящиеся в банковских офисах. Еще встречается использование мошенниками реквизитов карты в интернете. Никому не сообщайте реквизиты своей банковской карты. Для совершения операций в интернете заведите отдельную карту с ограниченным лимитом и используйте известные, проверенные сайты. К сожалению, периодически появляются все новые и новые способы мошенничества с банкоматами, например, установка фальшивого банкомата», — рассказывает господин Климов.

Эксперты считают, что некоторые виды финансовых махинаций оказывают самое негативное влияние на кредитные организации и общество.

К примеру, Роман Гринченко, аналитик «Инвесткафе», говорит, что основную опасность представляют финансовые пирамиды, так как для финансово неграмотных граждан они выглядят очень привлекательно, но при этом наносят ущерб кредитным организациям. «Причиной ущерба является то, что люди, участвующие в пирамидах, берут кредиты, а когда пирамида рухнет, берут кредиты для погашения кредитов, что в итоге способствует росту объемов просроченных задолженностей.

Также стоит отметить привлечение кредитов по фальшивым или чужим документам, что также приводит к росту количества невыплаченных кредитов. Основным залогом безопасности является доскональное изучение подписываемых бумаг, так как чаще всего мошенники для легализации махинаций прописывают условия в договоре, а невнимательные граждане не обращают на них внимание. Еще стоит сопоставлять доходность и риски, так как большинство мошенников обещают высокий доход и отсутствие рисков, что изначально должно настораживать», — говорит он.

ХВАТИТ ДЕРЖАТЬ ПИН-КОДЫ В КОШЕЛЬКАХ

По словам госпожи Лихицкой, никогда не стоит звонить по незнакомым номерам, пришедшим в непонятном SMS-сообщении или отправлять какие-либо данные в ответ на SMS-запросы с незнакомых номеров. «И обязательно подключайте услугу SMS-информирования по пластиковой карте, чтобы иметь возможность отследить любые несанкционированные операции по снятиям или переводам на своих банковских картах», — говорит она.

По словам госпожи Ванчиковой, для того чтобы обезопасить себя от мошенников, нельзя сообщать свои данные малознакомым лицам, стараться по возможности избегать ненужного ксерокопирования документов, не регистрироваться без необходимости на каких-либо сайтах. «В случае утраты паспорта, который является основным документом, удостоверяющим личность, нужно немедленно обратиться в органы УФМС и сообщить об утрате. Время от времени проверять записи своей кредитной истории, один раз в год любой гражданин может это сделать бесплатно. Кроме того, банки рекомендуют пользоваться дистанционными сервисами, которые позволяют контролировать состояния счетов в режиме реального времени: интернет-банк, мобильный банк и SMS-уведомление», — дает несколько советов Галина Ванчикова.

По мнению госпожи Зайцевой, наиболее актуальными инициативами, направленными на снижение уровня преступлений в данном сегменте, остаются развитие информационных программ для населения и дальнейшая оптимизация нормативной базы, направленная на повышение защиты интересов потребителей этих услуг. «В совокупности реализация широкого спектра мер такого характера должна повышать уровень доверия населения в целом к финансовому рынку и безналичными операциям в частности, способствовать росту индустрии банковского процессинга и дистанционных платежей», — выражает надежду она.

Госпожа Магерио говорит, что перед тем как воспользоваться банкоматом, особен-

но находящимся вне банковского офиса, необходимо проверить его на отсутствие в нем скимминговых устройств. «Мошенники устанавливают их на гнездо банкомата, которое принимает банковскую карту, чтобы считать данные вашей карты. Перед вводом пин-кода в банкомате осмотрите клавиатуру на наличие на ней каких-либо дополнительных накладок. Всегда закрывайте банкомат и клавиатуру корпусом и рукой при вводе пин-кода», — предостерегает госпожа Магерио.

Владимир Климов рассказывает, что против мошенничества с картами помогает соблюдение простых мер предосторожности. «Не оставляйте карту без присмотра, не передавайте карту третьим лицам, не используйте ее в подозрительных местах. Сейчас многие банки размещают круглосуточно работающие банкоматы в зонах с видеонаблюдением — предпочтительнее пользоваться банкоматами, находящимися в банковских офисах или именно в таких зонах. Никогда не записывайте пин-код, а если вы это сделали, храните карту и пин-код отдельно. И если вы еще не подключили услугу SMS-уведомлений о транзакциях по карте, необходимо сделать это — данная функция позволит отслеживать все движения по карте и незамедлительно получать информацию об этом», — говорит он.

Что касается пользования банкоматами, то, по словам господина Климова, следует преимущественно пользоваться известными клиентам банкоматами в привычных местах. «Отдавайте предпочтения тем банкоматам, которые установлены в отделениях банков. Обращайте внимание на внешний вид банкомата. Серьезные банки следят за внешним видом своих устройств, и они, как правило, соответствуют корпоративному стилю. Мошенники зачастую пренебрегают такими вещами, выявленные случаи размещения фальшивых банкоматов это подтверждают. Обращайте внимание на то, какому банку принадлежит банкомат. Если банк вам совсем не знаком, воздержитесь от использования такого устройства», — советует господин Климов. ■