КАРТЫ, ДЕНЬГИ В ДВА СЧЕТА

С НАЧАЛА 2019 ГОДА ГУ МВД ПО ПЕРМСКОМУ КРАЮ ЗАРЕГИСТРИРОВАЛО ПОЧТИ 4,5 ТЫС. ПРЕСТУПЛЕНИЙ, КОТОРЫЕ СОВЕРШЕНЫ С ПОМОЩЬЮ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ. В ПОДАВЛЯЮЩЕМ БОЛЬШИНСТВЕ СЛУЧАЕВ ОНИ СВЯЗАНЫ С ХИЩЕНИЕМ СРЕДСТВ С БАНКОВСКИХ СЧЕТОВ ЮРИДИЧЕСКИХ И ФИЗИЧЕСКИХ ЛИЦ. И ЕСЛИ РАНЬШЕ ПРЕСТУПНИКИ ИСПОЛЬЗОВАЛИ ТОЛЬКО ТЕЛЕФОНЫ, ТО СЕЙЧАС ИМ ДОСТУПНЫ МЕССЕНДЖЕРЫ И СПЕЦИАЛЬНО РАЗРАБОТАННЫЕ ПРОГРАММЫ И ВИРУСЫ. КАК ЛЮДИ СТАНОВЯТСЯ ЖЕРТВАМИ ЗЛОУМЫШЛЕННИКОВ И КАК С ПОСЛЕДНИМИ БОРЮТСЯ ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ, РАЗБИРАЛСЯ КОРРЕСПОНДЕНТ BG. ДМИТРИЙ АСТАХОВ

ОЛЕГ ХАРСЕЕВ

ПО МЕРЕ РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ УВЕЛИЧИВАЕТСЯ ЧИСЛО СХЕМ МОШЕННИЧЕСТВА

ИНЖЕНЕРЫ СЧЕТОВ ЧЕЛОВЕЧЕСКИХ

Телефонным мошенничеством традиционно занимались «постояльцы» исправительно-трудовых учреждений, которые часто наугад набирали номера и убеждали доверчивых людей перевести деньги с банковского счета или, реже, передать посредникам. Некоторые из них оказались настолько успешны в этой деятельности, что даже решили выйти на «международный рынок» и пытались нанять преподавателей иностранных языков для занятий по Skype. В терминологии работников информационной безопасности банковской сферы злонамеренное введение в заблуждение клиентов банка с целью хищения средств называется «социальной инженерией».

С развитием информационных технологий выросли и возможности «инженеров». По словам начальника отдела безопасности и защиты информации Пермского отделения Уральского ГУ Банка России Михаила Теплоухова, в последнее время телефонные мошенники в качестве канала связи используют IP-телефонию. Она позволяет им создавать подменные номера, идентичные call-центрам банков. При этом номера мобильных телефонов клиентов банка злоумышленники могут получать из похищенных баз данных, которые продаются в теневом сегменте интернета.

За первые шесть месяцев 2019 года Центробанком обнаружено более 12 тыс. объявлений о продаже баз данных, 12% из них относились к базам, касающимся кредитно-финансовой сферы.

«Чаще всего ситуация выглядит следующим образом,— рассказывает Михаил Теплоухов.— Клиент банка получает звонок с номера, идентичного номеру call-центра кредитной организации, указанному на оборотной стороне карты. Вежливый собеседник называет его по имени-отчеству и представляется сотрудником службы безопасности банка. Дальше следует убедительная история о том, что зафиксирована попытка снятия средств со счета и необходимо выполнить ряд действий, которые заключаются в том числе в предоставлении данных о банковской карте, а также CVC и CVV кодов. В результате человек лишается своих денег».

Мошенники, как правило, владеют профессиональной терминологией работников банковской сферы и техниками убеждения. В Центробанке отмечают, что в подобных случаях не стоит вступать в разговор, тем более что при наличии каких-то сомнений служба безопасности банка сама никогда не звонит. Получив данные о попытке проведения нетипичных операций, система мониторинга блокирует карту автоматически.

Центробанк РФ фиксирует также рост количества сайтов (почти в семь раз за первое полугодие), использующихся для хищения средств владельцев карт. Они предлагают бесплатно получить компенсации, выигрыши, дешевые товары, для чего требуется ввод данных карты. За полгода по инициативе ЦБ было разделегировано более 9,7 тыс. фишинговых доменов, что фактически исключает техническую возможность работы таких сайтов на территории страны. Это спровоцировало переход владельцев сайтов в иностранные доменные юрисдикции. Их блокировка занимает гораздо больше времени.

Аналитики Центробанка обращают внимание и на новый всплеск активности нелегальных или псевдоброкерских организаций, которые работают на рынке «Форекс». Таких за девять месяцев текущего года выявлено более 140. Одна подобная организация установлена в Пермском крае. Как правило, их сотрудники предлагают желающим поиграть на бирже с помощью специального сайта или приложения. Но часто такая игра оказывается лишь имитацией через «нарисованный» сайт, никак не связанный с брокерскими платформами. Поэтому возможности заработать денег на сделках у человека нет.

Тенденция 2019 года — открытие «обучающих центров», которые предлагают подготовку аналитиков и учат работать на рынке ценных бумаг. Деятельность одного из таких центров минувшим летом выявили сотрудники Центробанка и пресекли оперативники ГУ МВД по Пермскому краю. Компания «Финмаркет» действовала по аналогичной схеме, предлагая сделать из обычных людей продвинутых биржевых аналитиков. Денег за «обучение» сотрудники компании не брали. Клиентам предлагали сначала сыграть на демосчете платформы Global Palace, а затем создать личный кабинет и продолжить играть самостоятельно, но уже за собственные деньги. «Инвестированные» средства сразу отправлялись на счета «Финмаркета», а «торги» вручную контролировал системный администратор сайта, который через какое-то время обнулял счет. По данному факту следственными органами было возбуждено уголовное дело по ч. 4 ст. 159 УК РФ (мошенничество в особо крупном размере).

«Самый главный момент, с которым нужно сразу разобраться при общении с брокерскими компаниями, есть ли у них лицензия Банка России на соответствующий вид деятельности,— отмечает Михаил Теплоухов.— Ее наличие легко проверить в открытых источниках. Если лицензии нет, то и отношений с ними иметь не стоит».

СТРАХОВОЧНЫЙ УЗЕЛ Впрочем, случаи обмана клиентов банка нередки не только со стороны мошеннических структур, но и со стороны сотрудников самих кредитных организаций. Ежегодно Центробанк регистрирует несколько тысяч обращений по поводу мисселинга — продажи финансового продукта или оказания услуги вместо тех, за которыми клиент обратился в финансовую организацию изначально и которые ему нужны на самом деле. С 2019 года жалобы такого рода регулятор выделил в отдельную категорию.