Информацию о новых способах мошенничества с банковскими картами регулярно публикуют и СМИ, и сами кредитно-финансовые учреждения, страдающие от мошенников наравне с клиентами. Однако находчивость преступников позволяет им снова и снова находить жертв среди доверчивых и невнимательных обывателей. 9111.ru вспомнил о самых распространенных способах мошенничества с банковскими картами.

Разблокировка карты по телефону

Одной из самых распространенных мошеннических схем является СМС-переписка или телефонные переговоры злоумышленников с пострадавшим от имени сотрудников банка. Так, 57-летней жительнице Великого Новгорода на телефон пришло сообщение о том, что ее платежная карточка заблокирована, а для ее разблокировки необходимо связаться по указанному номеру с менеджером службы поддержки.

Доверчивая пенсионерка позвонила по телефону, и на другом конце приятный мужской голос попросил продиктовать ему данные карты, включая пин-код. После того, как необходимые сведения были получены, мошенник заверил пострадавшую, что проблема устранена. Вскоре женщина обнаружила пропажу с банковского счета более 200 тыс. рублей.

Разблокировка карты – наиболее распространенный, но не единственный повод обратиться к владельцу банковской карты от имени, внушающего доверие лица или учреждения с целью получения конфиденциальной информации. Фантазия у злоумышленников работает хорошо. Так, в апреле 2016 года мошенник позвонил жительнице Нижнего Новгорода и представился руководителем отдела выплат одной из частных компаний. Обманным путем он узнал у женщины код авторизации для входа в личный кабинет мобильного приложения ее банка. Затем со своего мобильного телефона зашел в приложение и перевел себе 99 тыс. рублей, находившиеся на карте владелицы.

До этого жертвой мошенника стала жительница Тольятти, у которой аналогичным образом было похищено 80 тыс. рублей. Подозреваемым оказался 26-летний уроженец Северной Осетии. Поймать его удалось лишь в марте 2017 года.

Помните, что официальный представитель банка в случае нештатной ситуации обязательно позвонит клиенту или отправит сообщение со специального номера, зарегистрированного на финансовую организацию. К примеру, у Сбербанка это трехзначный номер 900. Этот номер должен быть знаком клиенту, потому что с него он обычно получает СМС-информирование о движении денежных средств на счете. Злоумышленники не смогут отправить СМС с этого номера. В любом случае, даже если звонит официальный представитель банка, ему нельзя сообщать пин-код, трехзначный CVV-код на обратной стороне карты, код авторизации, присланный по СМС, логин и пароль от личного кабинета в интернет-банке. Такую информацию могут запрашивать только мошенники.

Банк списал деньги с карты – как вернуть?

Вирус в телефоне съест деньги с карты

Еще один вид мошенничества разработан знатоками всевозможных компьютерных примочек. Хакеры заражают смартфон вирусной программой, которая получает

доступ к персональным данным владельца. Нередко она проникает на мобильное устройство вместе с каким-нибудь бесплатным приложением или через СМС.

Если на телефоне установлен мобильный банк, вирус может с помощью команд смс-банкинга сделать перевод средств с карты. При этом владелец даже не заподозрит неладное, так как все произойдет для него незаметно. Вредоносная программа сама совершит перевод и сама же подтвердит от имени потерпевшего операцию.

Так, 26-летний мужчина, отбывающий наказание в одном из исправительных учреждений города Ангарска, распространял через СМС-сообщения вирусную программу. Открывая ее, владельцы заражали свои мобильники вредоносным «шпионом», который похищал их деньги. Жертвами мошенника стали, по меньшей мере, 19 россиян, проживающих в разных регионах. В настоящее время точное число пострадавших уточняется, возбуждено уголовное дело.

В целях безопасности владельцам смартфонов, «привязавших» банковскую карту к телефону либо установивших мобильное приложение интернет-банка, рекомендуется пользоваться антивирусом, скачивать приложения только из официальных магазинов APP Store и Google Play, не переходить по ссылкам из СМС.

Скиммеры в банкомате

Нередко преступники используют для кражи данных специальные устройства, которые незаметно крепятся на банкомат и считывают секретную информацию с карт клиентов. Называются такие шпионские штучки скиммерами. Прибор копирует данные с магнитной полосы карточки владельца, когда та оказывается в слоте. А с помощью накладной клавиатуры или незаметной мини-камеры мошенники фиксируют вводимый пин-код.

Впоследствии данные «заливаются» на карту-пустышку, с которой снимаются деньги пострадавшего. Так, в Казани, по данным МВД, от рук двух мошенников скиммеров пострадали 57 человек. Установленную ими аппаратуру удалось обнаружить, только когда банкомат вскрывал мастер. Камера скиммера отвалилась, так как была прикреплена на двустороннюю застежку-липучку. После этого было возбуждено уголовное дело.

Сейчас в России используются карты, оснащенные чипами, поэтому актуальность скимминга в последнее время снизилась. По данным одного из крупнейших банков РФ, в 2013 году на долю таких операций приходилось до 50% хищений от общего объема всех денежных средств, сегодня эта цифра не превышает 7%.

Однако ЦБ предупреждает, что в ближайшее время страну может захлестнуть новая волна подобного мошенничества. Поскольку усовершенствованное оборудование позволяет преступникам считывать информацию даже с защитных чипов. Самыми проблемными регионами с точки зрения мошенничества с банковскими картами являются Москва, Московская область и Санкт-Петербург.

Как воруют деньги у Вас и Ваших детей с мобильных телефонов?

Деньги на липучке

Еще один распространенный способ отъема денег через банковские терминалы – это липучки. Человек пытается снять деньги, производит все обычные для этого операции с банкоматом, уже слышит характерный шум отсчитываемых купюр со стороны диспенсера, но наличность машина почему-то не выдает. Обычно такое списывается

на неисправность банкомата, и держатель карты направляется к другому устройству. Но деньги в действительности со счеты снимаются, но застревают в слоте для наличности благодаря помещенному туда двустороннему скотчу-липучке. В последствии их забирает мошенник.

В 2015 году в Нижнем Новгороде задержали 32-летнего мужчину, обвиняемого в хищениях денег из банкомата. Злоумышленник вместе с подельниками устанавливал на пластину корпуса терминала для выдачи денег липкую закладку. Преступники оставались неподалеку и наблюдали за жертвами. Когда клиент банка вносил или снимал какую-то сумму с карточки, деньги прилипали к закладке. После того, как растерянный гражданин уходил ни с чем, мошенники возвращались к банкомату и забирали наличность. Задержать подозреваемых удалось благодаря камерам видеонаблюдения, правда, чтобы установить личности злоумышленников, полицейским потребовалось немало времени.

Что делать, если банкомат «украл» деньги?

Бесконтактная кража

У некоторых держателей карт не так давно появилась функция бесконтактной оплаты покупок: PayWave (Visa) или PayPass (MasterCard). Для того, чтобы оплатить товар, необходимо просто приложить карту к считывающему устройству на кассе, и деньги будут списаны автоматически. Предприимчивые преступники решили заработать на нововведении и теперь незаметно крадут средства с банковских карт в людных местах.

Злоумышленники прислоняют специальный считыватель или POS-терминал к карману или сумке жертвы, где лежит бесконтактная карточка, и списывают суммы в пределах установленного лимита. Для небольших операций не нужен пин-код, этим и пользуются воры.

На Сахалине жертвой такого вида мошенничества стал 23-летний местный житель. Он остался без денег после обычной поездки в автобусе. Неизвестные сняли с его счета 8 000 рублей, прислонив специальный прибор к карману с кошельком. Полиция региона уже забила тревогу, предупреждая, что новый способ отъема денег у населения в последнее время набирает обороты. В данном случае жертвами мошенников могут стать даже самые бдительные граждане. Чтобы сохранить кровные, эксперты советуют хранить карты с технологией бесконтактной оплаты завернутыми в фольгу или в специально разработанных для них кошельках. Другого способа противостоять этому виду мошенничества пока не придумали.

Данная стать взята с сайта www.9111.ru

Уважаемые жители Николаевского сельского поселения!

Просим Вас немедленно сообщать о случаях социальных мошенничеств в:

Отдел МВД по Константиновскому району по тел. 2-16-11, Участковому УПП Демину А.В. по тел.89994711524

Прокуратуру Константиновского района по тел. 2-15-95