Схемы мошенничества

Сохранность денежных средств клиента, сохранность банковской карты и/или ее реквизитов во многом зависит от самого держателя карты, от его знаний правил пользования картой, соблюдении им мер безопасности при проведении операций с использованием карты, а также информированности о схемах мошенничества с банковскими картами, используемых преступниками.

Наиболее распространенными схемами мошенничества с банковскими картами являются следующие:

Интернет-мошенничество на доверии – это самая распространенная в настоящее время схема мошенничества, которая может выглядеть следующим образом:

На телефонный номер держателя карты, разместившего в газете или на сайте публичное объявление о продаже того или иного имущества, поступает звонок от якобы потенциальных покупателей с целью приобрести данное имущество. После чего «потенциальный покупатель» предлагает удобную форму оплаты в виде пополнения банковской карты, для чего просит сообщить ему такие данные банковской карты, как номер карты, срок действия, проверочный код, а также дополнительный секретный код, направляемый банком в SMS-сообщении на мобильный телефон клиента при совершении клиентом операции в сети Интернет. Получив данную информацию, «потенциальный покупатель» совершает не операцию пополнения карточного счета клиента, а операцию по переводу/списанию денежных средств в сети Интернет с карты держателя, например, на свой электронный кошелёк.

Мошенники представляются службой безопасности банка и сообщают клиенту о подозрительной операции по его карте и о возможности вернуть якобы списанные с карты деньги. Либо сообщают о сбое в системе банка и необходимости блокировать карту. Для решения проблемы мошенники просят сообщить данные карты, пароли от мобильного банка. При этом злоумышленники с помощью современных технологий используют подмену

номеров телефонов под официальные номера банка, тем самым усыпляя бдительность клиента.

Мошенники сообщают, что с банковской картой клиента или мобильным приложением произошел некий инцидент, и убеждают установить приложения, якобы защищающие денежные средства. Такие приложения могут оказаться программами удаленного доступа и управления устройством клиента: TeamViewer, AnyDesk или их аналоги. После установки такой программы и получения ID и кодов доступа мошенники подключаются к устройству жертвы и могут управлять им, просматривать любую информацию, выполнять операции через мобильный банк.

Мошенники активно используют тему коронавирусной инфекции и состояние обеспокоенности людей для хищения денежных средств. Злоумышленники могут представиться работниками Пенсионного фонда, Роспотребнадзора и других государственных или социальных организаций, сообщить о положенной социальной выплате или материальной помощи, тем самым вынуждая предоставить информацию о карте, кодах, паролях из смс, персональных данных, либо совершить какие-либо действия для получения выплат.

Оставление карты в банкомате – в случае применения этой новой схемы мошенники якобы случайно забывают карту в банкомате и просят ее изъять оказавшегося рядом человека. После того, как тот берет карту, злоумышленник проверяет ее баланс и утверждает, что с его счета пропали деньги и вынуждает вернуть доставшего карту человека эту сумму. В используемой злоумышленниками схеме могут участвовать двое или трое — еще один человек будет изображать «свидетеля» кражи денег с карты. Притворившийся пострадавшим злоумышленник начнет угрожать вызвать полицию, обосновывая это тем, что на его карте остались чужие отпечатки пальцев, и якобы будет легко доказать предполагаемую пропажу денег с карты.

На самом же деле никакой кражи денежных средств от прикосновения к карте не происходит, мошенники пытаются заполучить денежные средства путем запугивания и обмана оказавшегося рядом человека.

Компрометация ПИН-кода держателем банковской карты. Под этим понимается запись ПИН-кода непосредственно на карте или на каком-либо носителе (лист бумаги, записная книжка, мобильный телефон), хранимом вместе с картой. Если банковская карта утеряна или украдена (обычно вместе с бумажником, барсеткой, сумочкой), то у вора оказывается и карта, и персональный код. В таком случае мошенникам совсем нетрудно несанкционированно использовать банковскую карту для получения наличных денежных средств и/или оплаты товаров (услуг).

Дружественное мошенничество. Член семьи, близкий друг, коллега по работе, имея доступ к месту хранения банковской карты, берет ее без разрешения ее держателя, а затем, предварительно узнав ПИН-код, использует карту в своих целях.

Подглядывание из-за плеча. Мошенник может узнать ПИН-код держателя банковской карты, подглядывая из-за его плеча, пока тот вводит свой код, осуществляя операции в банкомате или в электронном терминале. При этом могут использоваться специальные оптические приборы. Затем мошенник осуществляет кражу карты и использует её в своих целях.

Фальшивые банкоматы. В последнее время преступники воспользовались ростом числа банкоматов и стали применять "фальшивые" банкоматы или прикреплять к настоящим банкоматам специально сконструированные устройства.

Мошенники разрабатывают и производят фальшивые банкоматы, либо переделывают старые, которые выглядят как настоящие. Они размещают свои банкоматы в таких местах, как, например, оживленные торговые районы, где ничего не подозревающие держатели банковских карт попытаются получить из таких фальшивых банкоматов деньги. После введения карты и ПИН-кода обычно на дисплее фальшивого банкомата появляется надпись, что денег в банкомате нет или что банкомат не исправен. К тому времени мошенники уже скопировали с магнитной полосы карты информацию о счете данного лица и его персональный идентификационный номер.

Копирование магнитной полосы (skimming). Данный вид мошенничества подразумевает под собой использование устройств, считывающих информацию с магнитной полосы банковских карт при ее использовании в электронных устройствах (банкоматах, электронных терминалах). Специально изготовленные клавиатуры, которыми накрывают существующие клавиатуры настоящих банкоматов/терминалов, для считывания конфиденциальных данных магнитной полосы, запоминания ПИН-кода.

Законный держатель банковской карты проводит операцию с вводом персонального идентификационного номера (ПИН), в это время дополнительно установленное устройство считывает и записывает информацию на магнитной полосе. Т.е. у злоумышленников появляется данные необходимые для дальнейшего изготовления поддельной карты и ее использования в своих целях.

Ложный ПИН-ПАД. Держателю карты может быть предложено ввести ПИН-код не в настоящий ПИН-ПАД (устройство для ввода ПИН-кода), а в ложное устройство его имитирующее, которое запомнит введенный код. Такие устройства иногда устанавливают рядом со считывающими датчиками, предназначенными для прохода в помещение с банкоматом с использованием в качестве идентификатора (электронного ключа) банковской карты.

Фишинг (англ. phishing) – измененная форма от английских слов phone (телефон) и fishing (рыбная ловля). Термин появился для обозначения схемы, в результате которой, путем обмана, становятся доступными реквизиты банковской карты и ПИН-код. Чаще всего используется в виде рассылки sms-сообщений о блокировании карты, успешном совершении операции перевода денежных средств или изменении настроек, а также рекомендация перезвонить на номер мобильного телефона с целью получения инструкций по разблокированию карты. Также могут быть использованы рассылки электронных писем от имени банка или платежной системы с просьбой подтвердить указанную конфиденциальную информацию на сайте организации. Фишинговое письмо может выглядеть следующим образом.

От: VISA Сервис [mailto:VisaService@visa.com]

Отправлено: дата, время

То: держатель карты

Тема: Внимание! Потеряна база данных кредитных карт VISA!

Здравствуйте, к сожалению, в виду того, что некоторые базы данных были взломаны хакерами, Visa установила новую систему безопасности. Вам следует проверить Ваш остаток, и в случае обнаружения подозрительных транзакций обратиться в Ваш банк-эмитент. Если Вы не обнаружите подозрительных транзакций, это не означает, что данные карты не потеряны и не могут быть использованы. Возможно, Ваш банк-эмитент еще не обновил информацию. Поэтому мы настоятельно рекомендуем Вам посетить наш Интернет-сайт и обновить Ваши данные, иначе мы не сможем гарантировать Вам возврат украденных денежных средств. Спасибо за внимание. Нажмите сюда для обновления Ваших данных.

Неэлектронный фишинг— его появление обусловлено увеличением объемов эмиссии микропроцессорных карт и связанной с этим процессом программой международных платежных систем «чип и ПИН», т.е. осуществление покупки в предприятии торговли (услуг) посредством обязательного ввода ПИН-кода. В отличие от традиционного— электронного фишинга (см. выше), в схемах неэлектронного фишинга создаются реальные торгово-сервисные предприятия/офисы банков либо используются уже существующие. Держатели платежных карт совершают покупки товаров, получают услуги либо снимают денежные средства в кассе банка. Операции производятся с использованием банковских микропроцессорных карт и сопровождаются введением клиентом своего ПИН-кода. Сотрудники мошеннических предприятий негласно копируют информацию с магнитной полосы карты и производят запись персонального идентификационного номера. Далее мошенники изготавливают поддельную банковскую карту, и в банкоматах производится снятие денежных средств со счета клиента. Данный вид мошенничества распространен в Турции, но может происходить и в других странах мира.

Вишинг (англ. vishing) – разновидность фишинга - голосовой фишинг, использующий технологию, позволяющую автоматически собирать

конфиденциальную, такую как номера карт и счетов информацию. Мошенники моделируют звонок автоинформатора, приняв который держатель получает следующую информацию:

автоответчик предупреждает, что с его картой производятся мошеннические действия, и дает инструкции – перезвонить по определенному номеру немедленно;

злоумышленник, принимающий звонки по указанному автоответчиком номеру, часто представляется вымышленным именем от лица финансовой организации и проводит идентификацию клиента, позволяющую узнать персональные данные клиента и карты;

либо на другом конце провода автоответчик, сообщающий, что человек должен пройти сверку данных, а также ввести 16-значный номер карты с клавиатуры телефона;

как только все необходимые данные получены, вишеры становятся обладателями информации (номер телефона, полное имя, адрес), которая может быть использована для совершения операций в сети Интернет;

затем, используя информацию, полученную в ходе первого звонка, можно собрать и дополнительную информацию, такую, как PIN-код, срок действия карты, номер банковского счета и т.п., что позволяет изготовить поддельную карту для использования в физических устройствах.

Фарминг (англ. "pharming" – производное от слов “phishing” – измененная форма от английских слов phone (телефон) и fishing (рыбная ловля) и "farming" – занятие сельским хозяйством, животноводством) — это процедура скрытного перенаправления пользователей на поддельные сайты. Злоумышленник распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения к заданным сайтам, в том числе обращения пользователя к сайту своего банка с целью управления своим банковским счетом, на поддельные сайты. Таким образом, обеспечивается высокая скрытность атаки, а участие пользователя сведено к минимуму – достаточно дождаться, когда пользователь решит посетить интересующие злоумышленника сайты. Попадая на поддельный сайт, пользователь для выполнения той или иной операции по своему счету, вынужден подтвердить

свои пароли и указать реквизиты банковской карты, которые тем самым становятся известны мошенникам.

В последнее время участились случаи телефонного мошенничества, при котором владельцы сотовых телефонов получают SMS сообщения недостоверного содержания, заманивающие пользователей на инфицированный веб-сайт. В тексте фальшивого SMS сообщения пользователю обычно сообщается о том, что он подписан на некую платную услугу, за которую ежедневно с его счета будет удерживаться определенная сумма, и если он хочет отказаться от данной услуги, то ему нужно зайти на сайт. Зайдя на указанный в SMS сообщении сайт, пользователь активирует троянскую программу, которая заражает компьютер и открывает тем самым мошенникам доступ к компьютеру пользователя. Такой тип мошенничества получил название смишинг (англ. "SMiShing" – производное от SMS и “phishing”).

Снифферинг (от английского to sniff – «вынюхивать») – это способ мошенничества, при котором злоумышленник использует анализатор проходящего трафика Интернет-сети («сниффер») – специальную компьютерную программу для перехвата данных с возможностью их декодирования и анализа. Снифферинг особенно популярен в людных местах, везде, где есть общедоступная сеть wi-fi.