Мошенничества с платежными картами

Банковская карта - это инструмент для совершения платежей и доступа к наличным средствам на счёте, не требующий для этого присутствия в банке. Но простота использования банковских карт оставляет множество лазеек для мошенников.

ФОРМА ЗАЯВЛЕНИЯ ПЛАТЕЛЬЩИКА (ПОТЕРПЕВШЕГО) В БАНК ПЛАТЕЛЬЩИКА (ПОТЕРПЕВШЕГО) ОБ ОТЗЫВЕ ПЛАТЕЖА, ВОЗВРАТЕ ДЕНЕЖНЫХ СРЕДСТВ И ОТКЛЮЧЕНИИ СИСТЕМЫ МОБИЛЬНЫЙ БАНК (приобщается)

ФОРМА СПРАВКИ ПО ФАКТУ ИНЦИДЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (приобщается)

Чтобы не стать жертвой злоумышленников при пользовании банковскими картами необходимо придерживаться следующих правил

- никому не сообщать пин-, CVC- или CVV- коды банковской карты и одноразовые пароли;

- в торговых точках, ресторанах и кафе все действия с банковской картой должны происходить в присутствии держателя карты. В противном случае мошенники могут получить реквизиты карты, либо сделать копию при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки;

- в случае потери банковской карты немедленно позвонить в банк для блокировки - это поможет сохранить денежные средства;

- подключить услугу смс-информирование - это обеспечит контроль за проведением любых операции по карте. При получении смс о несанкционированном списании средств со счета, заблокировать карту;

- установить лимит выдачи денежных средств в сутки и за одну операцию (это можно сделать в отделении банка или удалённо - в интернет-банке). Мошенники не смогут воспользоваться сразу всей суммой, которая находится на карте;

- при вводе пин-кода прикрывать клавиатуру. Вводить пин-код быстрыми отработанными движениями - это поможет в случае, установки скрытых видеокамер мошенников;

- выбирать для пользования терминалы и банкоматы, которые расположены непосредственно в отделениях банка или других охраняемых учреждениях;

- использовать банковскую карту в торговых точках, не вызывающих подозрений;

- перед тем как вставить карту в картоприемник внимательно осмотреть банкомат на предмет наличия подозрительных устройств, проверить, надежно ли они закреплены. Если очевидно, что накладное устройство смонтировано кустарно (можно увидеть остатки клея, ненадежность конструкции и неравномерность крепления), то необходимо

позвонить на горячую линию банка, сообщить о данном факте и воспользоваться другим банкоматом;

- в случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - рекомендуется отказаться от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

Пришло СМС от банка о блокировке карты или звонят из банка и спрашивают номер карты, пароль и код доступа. Что делать?

Этот способ мошенничества является наиболее новым. Злоумышленники оформляют облачную АТС на одноразовую сим-карту, а затем через веб-интерфейс меняют телефонный номер своей станции на телефонный номер банка. Представляясь сотрудниками банка, преступники обзванивают клиентов и под различными предлогами выясняют у них номера карт, одноразовые пароли и коды доступа, необходимые для проведения операций по банковским картам. Также с номера-двойника банка мошенники массово рассылают клиентам банка смс-сообщения о блокировке карты. Для разблокировки им предлагают перевести деньги на счет или отправить смс-сообщение на короткий номер.

ПРИМЕР: Сообщение «Ваша банковская карта заблокирована». Предлагается бесплатно позвонить на определенный номер для получения подробной информации. Когда жертва звонит по указанному телефону, ей сообщают, что на сервере, отвечающем за обслуживание карты, произошел сбой, а затем просят сообщить номер карты и ПИН-код для ее перерегистрации.
На самом деле злоумышленникам нужен номер карты жертвы и ПИН-код. Как только потерпевший их сообщает, преступники получают возможность управлять счетом.
Для граждан: не сообщать реквизиты карты никому. Представители банка их знают! Ни одна организация, включая банк, не вправе требовать ПИН-код! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.

Фишинг и поддельные ("зеркальные") сайты

Фишинг - кража любых персональных данных, владение которыми позволяет преступникам получать выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для входа в электронную почту, платежную систему и аккаунты в социальных сетях. Персональную информацию мошенники используют для получения доступа к аккаунтам, к которым привязаны банковские карты, что позволяет похищать с их счетов денежные средства.

Для кражи персональных данных фишеры массово рассылают электронные письма от имени государственных органов или известных компаний, например, крупных банков или онлайн-магазинов. Их цель - заставить получателей перейти по указанной в письме ссылке на поддельный сайт компании, интерфейс которого внешне не отличим от настоящего сайта, и ввести свои личные данные. Для привлечения внимания к письму в теме указывается на перспективу большой выгоды или на проблему, требующую срочного разрешения.

Подставные страницы действуют недолго - как правило, не более одной недели, ввиду частого обновления базы антифишинговых программ и фильтров. Однако мошенники,

следуя отлаженной схеме, создают всё новые и новые сайты-фальшивки для сбора персональных данных.

Так, спамеры активно рассылали по всему миру фальшивые уведомления о выигрыше в лотереях, приуроченных к Чемпионату Европы по футболу, Олимпиаде в Бразилии и Чемпионатам мира по футболу в 2018 и 2022 годах. Для получения денег получателю письма предлагалось ввести на сайте несуществующей лотереи персональную информацию.

Данный способ возможен, когда потерпевший пользуется **«личным кабинетом»** на сайте банка. Преступниками создается сайт, адрес которого и внешнее оформление страниц трудноотличимы от официального сайта банка. Если потерпевший при входе на сайт банка не использует сохраненную ссылку, а просто в поисковой системе набирает название банка, то ему обычно предлагается несколько вариантов. Если потерпевшим будет осуществлен выход на «зеркальный сайт», то вводимыми данными для входа в личный кабинет банка (логин и пароль), могут воспользоваться злоумышленники и войти на настоящем сайте от имени потерпевшего в его личный кабинет. Далее возможен перевод денег со счета потерпевшего из личного кабинета или подключение к его счету услуги «мобильный банк» на любом абонентском номере.

Примеры:

Оформление полиса ОСАГО

- Мошенники регистрируют доменное имя, содержащее в названии слово «osago» или напоминающее доменное имя одной из известных страховых компаний. На этом домене размещается фишинговый сайт, страницы которого практически полностью копируют оформление оригинального веб-ресурса, принадлежащего страховой компании. Для расчета стоимости страхования пользователю необходимо заполнить небольшую анкету - указать имя, дату рождения, номер водительского удостоверения, данные об автомобиле, номер телефона и электронную почту для связи. После введения данных покупателю предлагают оплатить электронный полис ОСАГО с помощью банковской карты: указать номер карты, дату окончания ее действия и CVC/CVV-код. Мошенники перенаправляют пользователя на поддельную страницу подтверждения оплаты, где просят ввести полученный от банка код подтверждения оплаты. В случае успеха злоумышленники обходят двухфакторную аутентификацию и получают деньги. **Аналогичную схему обмана можно встретить при покупке авиабилетов онлайн.**

- Жители России получали письма, замаскированные под уведомления от Федеральной налоговой службы и Пенсионного фонда РФ, примерно следующего содержания: «Уважаемый налогоплательщик! У вас выявлена задолженность. Срок погашения долга до 23.12.2016 г. Подробнее Вы можете ознакомиться, перейдя по ссылке… » или «Осуществлен перерасчет пенсионных накоплений. Обязательно ознакомьтесь по ссылке…». После перехода на поддельный сайт государственного органа для получения более подробной информации пользователю предлагалось ввести свои персональные данные.

ВНИМАНИЕ: Основным признаком, что клиент зашел на «зеркальный» сайт банка является то, что **после ввода логина и пароля на странице появляется надпись о техническом обслуживании сайта или любая информация, в которой будет указано о том, что обратится на сайт можно позднее**. При этом на телефон не поступает СМС-сообщение от банка о входе в личный кабинет, если такая форма оповещения

предусмотрена.
Совет гражданам: при наступлении вышеописанных событий незамедлительно обратиться в банк по телефону горячей линии и заблокировать счет. Разблокировать его со сменой пароля можно при личном обращении в отделение банка с паспортом и картой.

Что такое "скимминг" (вид мошенничества с платежными картами)?

Считывание данных карты при помощи устанавливаемого на банкомат специального устройства (скиммера). С помощью него злоумышленники копируют информацию с магнитной полосы карты (имя держателя, номер и срок действия карты). Для считывания пинкода преступники устанавливают на банкомат миниатюрную камеру или накладку на клавиатуру.

Завладев информацией о карте, мошенник изготавливает ее дубликат и распоряжается денежными средствами держателя оригинальной карты.