НОВЫЕ ВИДЫ МОШЕННИЧЕСТВА С БАНКОВСКИМИ КАРТАМИ

С развитием новых технологий способы мошенничества с банковским картами также становятся более технологичными, появляются новые более «продвинутые» способы обмана. Если раньше карманника можно было просто поймать за руку, то теперь сделать это намного труднее, а иногда и совсем невозможно.

Мы не пугаем Вас – банковской картой вполне можно пользоваться безопасно, просто всегда нужно быть в курсе возможных видов мошенничества, чтобы подстраховаться от них. Как показывает практика, подавляющее большинство случаев мошенничества происходит по причине грубого нарушения владельцем карты элементарнейших правил безопасного пользования картой.

СМС-мошенничество

Суть данного вида мошенничества заключается в том, что мошенники наугад рассылают по всей имеющейся у них базе мобильных номеров SMS-сообщения, которые заставляют держателя карты понять, что:

- с картой что-то не в порядке (типа «Ваша карта заблокирована. Для разблокировки обратитесь по телефону Х»);
- по его карте проведена какая-то операция на определенную сумму (типа «Спасибо. Ваша заявка на перевод с карты 5000 рублей принята»);
- у Банка в результате технического сбоя возникли проблемы с базой данных клиентов и его просят для восстановления базы перезвонить и сообщить все свои персональные данные;
- на карту была зачислена или списана какая-то сумма денежных средств и т.п.

Внизу сообщения обычно приводится номер мобильного телефона, по которому настоятельно рекомендуют перезвонить, чтобы решить проблему. Обычно это простой незамаскированный номер мобильного телефона мошенника.

Иногда мошенники предлагают держателю карты зарегистрироваться на указанном в сообщении сайте, заполнить анкету и принять участие в розыгрыше ценных призов.

ВО ВСЕХ ЭТИХ СЛУЧАЯХ ЗАПОМНИТЕ - Банк никогда не посылает такого рода СМС-сообщений!

От Банка вы можете получать только следующие СМС:

- с номера **MULTICARTA** с идентификатором **LantaInfo** внутри сообщения**,** если подключены к услуге СМС-сервис (автоматическое получение СМС-уведомлений обо всех приходных и расходных операциях по карте);
- от системы интернет-банкинга HandyBank (если подключены к этой системе) с одноразовыми кодами для подтверждения проводимых вами операций.

Если Вы получили мошенническое сообщение с любого другого номера, то просто никак не реагируйте на него и удалите его. Если же Вас все-таки терзают сомнения, то перезвоните, НО не по указанному в сообщении номеру, а по номеру круглосуточной службы поддержки, указанному на обороте карты **((495) 785-15-15 или 8-800-200-30-22)**, либо по телефону Банка **(495) 957-00-67** (в рабочее время), и сотрудники службы поддержки снимут все ваши сомнения.

Цель мошенников – любым способом выйти на связь с Вами по телефону и получить от Вас конфиденциальную информацию или даже заставить вас под своего рода словесным гипнозом сделать какие-то конкретные действия с вашей картой – например, подойти к ближайшему банкомату и нажать «для проверки» те кнопки, которые они вам продиктуют. В результате вы можете сделать перевод денежных средств на указанную ими карту или пополнить мобильный телефонный номер мошенника и потерять все свои деньги.

Кардинг и Скиминг

Кардинг — род мошенничества (один из самых вредоносных видов хакерства), при котором производится операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Частным случаем кардинга является скимминг.

Скиминг — разновидность мошенничества с пластиковыми картами, при котором используется скиммер — инструмент злоумышленника для считывания магнитной дорожки платежной карты и последующего изготовления ее дубликата (чаще всего так называемого «белого пластика»).

Для получения копии банковской карты необходимо скопировать код карты с магнитной полосы карты и ПИН-код. Для этого мошенники устанавливают на банкомат перед или внутри слота для карты считывающее устройство — скиммер, который копирует код карты с магнитной полосы. Уникальный ПИН-код может фиксироваться с помощью миниатюрной видеокамеры, которую устанавливают на банкомат и направляют на клавиатуру ввода, или с помощью фальшивой накладной клавиатуры, которая запоминает вводимый код и последовательность набора цифр. Скиммер, мини видеокамера или фальшивая накладка клавиатуры, питаются от собственного источника энергии — миниатюрной литиевой батарейки. Все устройства изготавливаются под цвет и конкретную модель банкомата, поэтому их трудно заметить.

Таким образом, вы вставляете карту в банкомат, скиммер считывает с нее данные, злоумышленники изготавливают копию карты и пользуются ею, снимая денежные средства с вашего счета. Отследить случаи скиминга вовремя практически невозможно.

В нашей стране актуальность проблемы скиминга возросла относительно недавно. На сегодняшний день совместно с нашими зарубежными коллегами пойманы десятки групп, имеющих отношение к такому роду мошенничества, ведутся работы в создании продуманной схемы расследования данного вида преступлений.

Чтобы избежать «банкоматного» скиминга необходимо проявлять бдительность. Ваша бдительность — лучшее оружие против мошенников нового поколения. Дело в том, что взломанный банкомат почти всегда можно обнаружить, проявив внимательность. Например, мошенники могут использовать накладную клавиатуру для считывания ПИН-кода, в таком случае она расположена выше корпуса банкомата и под накладной клавиатурой виднеется часть оригинальной.

Внимательно смотрите на наклейку «вставьте карту», если она частично закрыта — банкомат взломан! Небольшое затемнение в слоте для приема — тоже может быть скиммером — устройством для считывания магнитного кода карты.

Ни в коем случае не стоит думать, что если вы вообще не пользуетесь сторонними банкоматами для снятия денежных средств, то проблема скиминга останется в стороне. Существуют и другие способы этого вида мошенничества.

Современный скиммер может иметь форму обычного мобильного телефона. Им могут пользоваться официанты, работники автозаправочных станций, продавцы магазинов, все, кто берет в руки вашу карту. Провести картой по скиммеру — дело нескольких секунд, а ПИН-код может считать скрытая камера или просто наблюдательный взгляд.

БУДЬТЕ БДИТЕЛЬНЫМИ ПРИ ПОЛЬЗОВАНИИ КАРТОЙ В ЛЮБЫХ ТОЧКАХ ОБСЛУЖИВАНИЯ!

- для снятия наличных пользуйтесь преимущественно банкоматами, установленными в отделениях банков. При снятии наличных через «чужие» банкоматы проверяйте их на наличие скиминг-устройств; Если банкомат кажется Вам подозрительным – лучше откажитесь от проведения операции и найдите другой банкомат;
- расплачиваясь за обслуживание в ресторанах никогда не упускайте из виду свою карточку, и тем более не отдавайте ее официанту, чтобы он на длительное время уносил ее куда-то для оплаты через терминал;
- прикрывайте рукой ПИН-клавиатуру при вводе вашего ПИН-кода в банкоматах и торговых терминалах;
- подключите услугу СМС-информирования об операциях с вашей картой и внимательно отслеживайте все входящие СМС-сообщения, чтобы немедленно заблокировать карту при начале мошеннических операций;
- знайте свое контрольное слово для идентификации при обращении в службу поддержки.
- имейте под рукой записанными в блокноте (или сохраненными в памяти своего мобильного телефона) номера телефонов **круглосуточной службы поддержки (495) 785-15-15, 8-800-200-30-22** или Отдела пластиковых карт Банка **(**только в часы работы Банка – (495) 957-00-67);

Если же вы все-таки стали жертвой обмана мошенников, то в кратчайший срок напишите заявление в Банк и ОВД по месту регистрации. Следуя этим рекомендациям, вы сможете минимизировать материальный ущерб и окажете содействие правоохранительным органам в оперативном поиске и задержании преступников.

НЕКОТОРЫЕ ПРИМЕРЫ УСТАНОВКИ СКИМИНГОВЫХ УСТРОЙСТВ НА БАНКОМАТЫ