Безопасность при пользовании банковской картой. Технические способы мошенничества

Авторы: Лобова Маргарита

2016

Цели и задачи

Цели:

Расширить знания банковских картах и безопасности их пользования

Раскрыть технические способы мошенничества

Задачи:

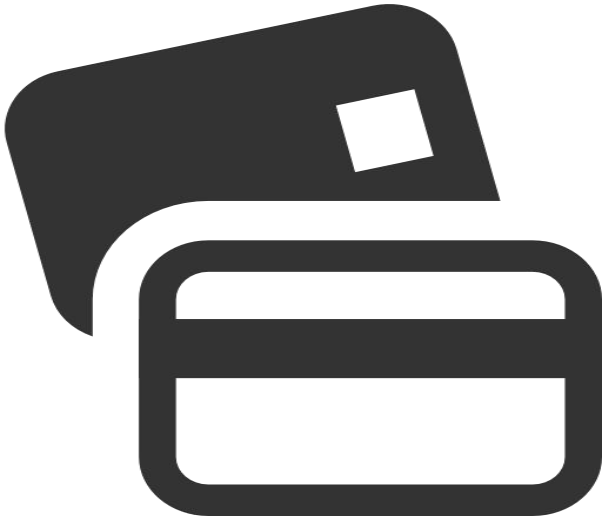
Получить сведения о банковских картах

Изучить способы защиты банковских карт

Изучить технические способы мошенничества

Банковская карта

- Ба́нковская ка́рта (англ. Bank Card, BCard, BC) — пластиковая карта, привязанная к одному или нескольким расчётным счетам в банке; инструмент, дающий возможность доступа к своему личному счету в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных.



Правила безопасного пользования картой

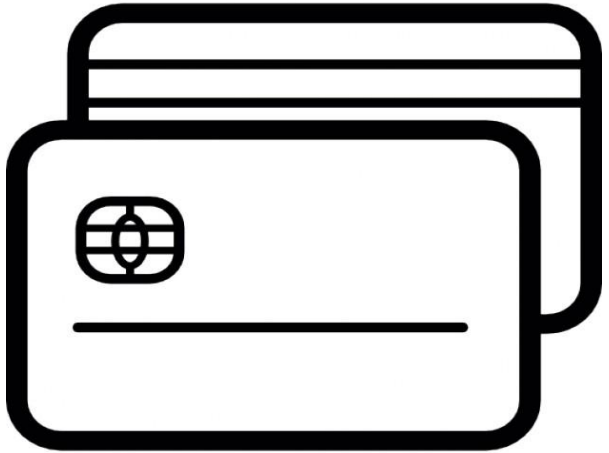
- Во избежание использования Вашей карты другим лицом храните ПИН-код отдельно от карты, не пишите ПИН-код на карте, не сообщайте ПИН-код другим лицам (в том числе родственникам), не вводите ПИН-код при работе в сети Интернет
- Во избежание мошенничества с использованием Вашей карты требуйте проведения операций с ней только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения

Правила безопасного пользования банковской картой

- Если к вам обратились по телефону, в интернете, через социальные сети или другими способами, и под различными предлогами пытаются узнать данные о вашей банковской карте, пароли или другую персональную информацию, будьте осторожны: это явные признаки мошенничества. При любых сомнениях рекомендуем прекратить общение и обратиться в банк по телефону, указанному на обратной стороне вашей банковской карты
- Не прислушивайтесь к советам третьих лиц, а также не принимайте их помощь при проведении операций. При необходимости обратитесь к сотрудникам в филиале банка или позвоните по телефонам, указанным на устройстве или на обратной стороне Вашей карты

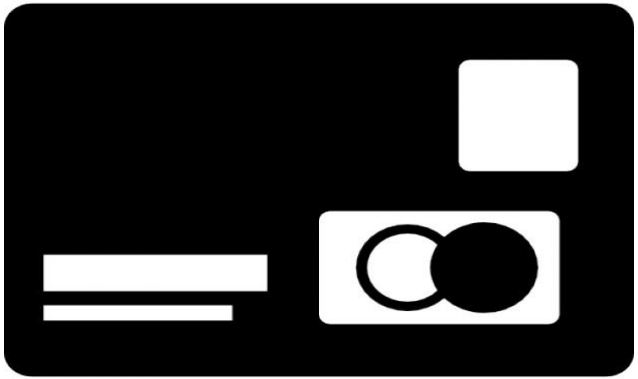
Правила безопасного пользования банковской картой

- Уничтожайте чеки с паролями от систем интернет-банка, если Вы не планируете их использование. Не передавайте чеки третьим лицам, в т. ч. сотрудникам банка
- Храните свою карту в недоступном для окружающих месте. Не передавайте карту другому лицу, за исключением продавца (кассира). Рекомендуется хранить карту отдельно от наличных денег и документов, особенно в поездках

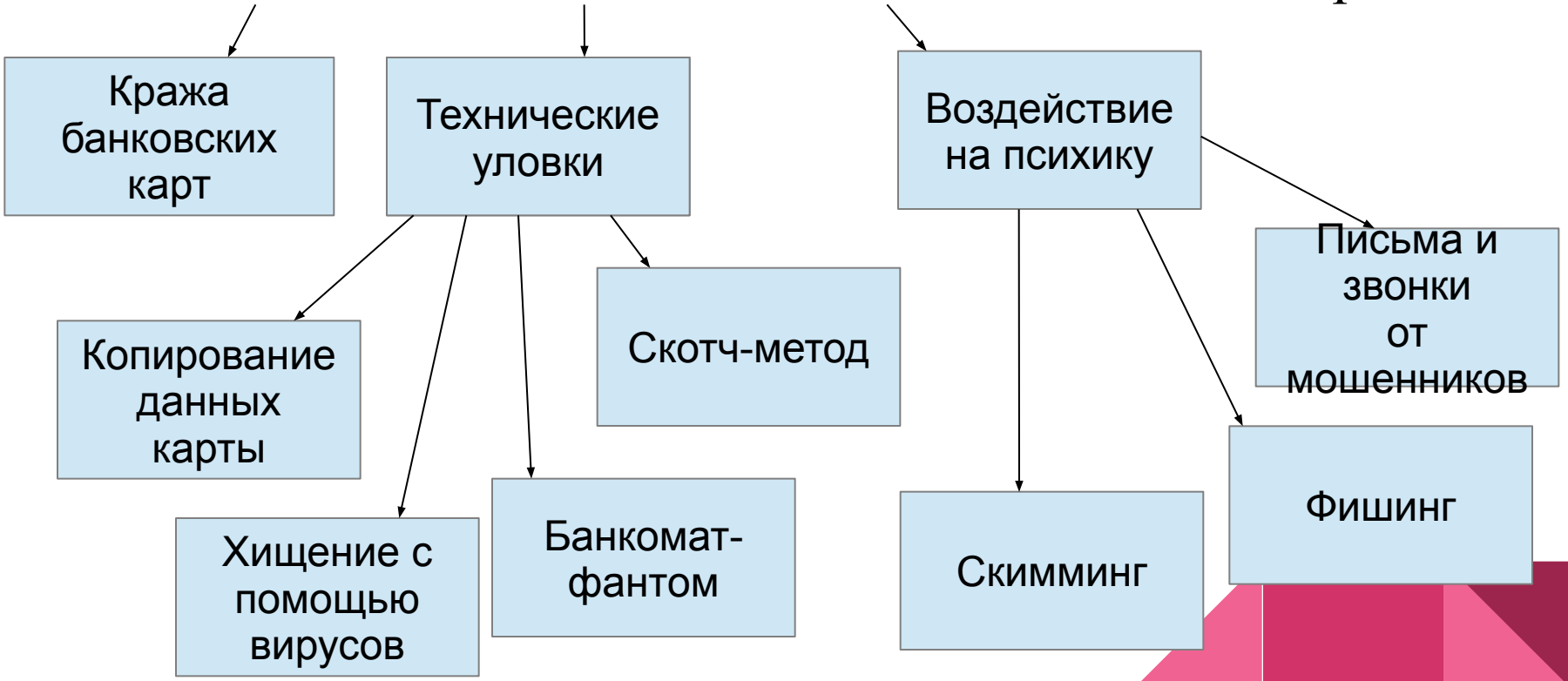


Мошенничество

- Мошенничество — хищение чужого имущества или приобретение права на чужое имущество путём обмана или злоупотребления доверием. Лицо, занимающееся этим, называется мошенник или мошенница.



Основные виды мошенничества с банковскими картами



Кража банковских карт

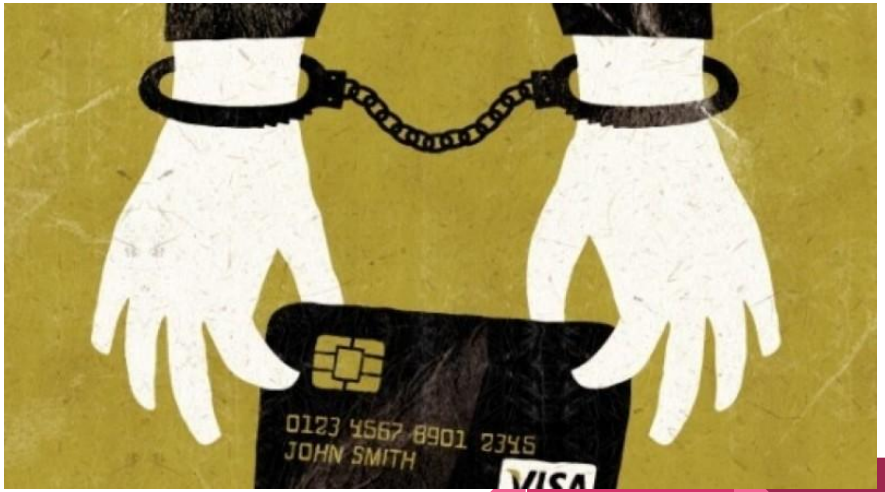
Кража — самый банальный способ мошенничества. У вас утащили кошелёк, а в нём несколько ваших карт, в том числе кредитных. Если все карты с чипом, тогда преступнику потребуется узнать пин-код, без которого в магазине не оплатишь товар, и деньги в банкомате не снимешь. Если там будет карта старого образца, её можно обналичить в магазине, купив любой товар.

Технические уловки.
Копирование данных карты работниками сферы обслуживания

Продавец или официант прокатывает вашу карту по специальному миниатюрному ручному скиммеру. Пин-код или другие реквизиты карточки легко фиксируются на видеокамеру, после чего также делается клон вашей карты и с неё снимаются деньги.

Хищение с помощью вирусов

- Весьма опасный вид технически-совершенного мошенничества, когда смартфон или компьютер «заражается» вирусной программой, например, троянцем (подробности в статье). Это настолько умный «цифровой вредитель», что может не только испортить данные на вашем компьютере или «утащить» ценную информацию, но и действовать от имени хозяина телефона (то ли ещё будет!).

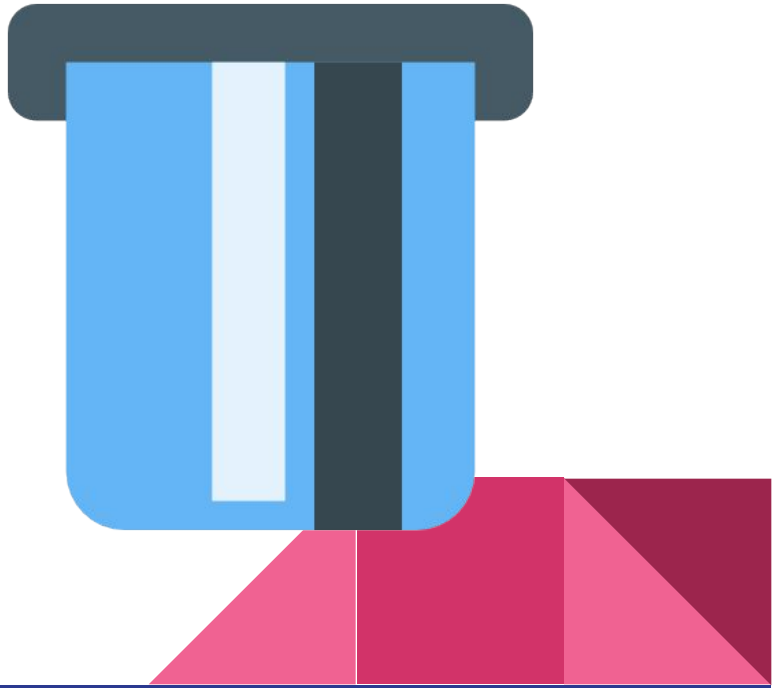


Хищение с помощью вирусов

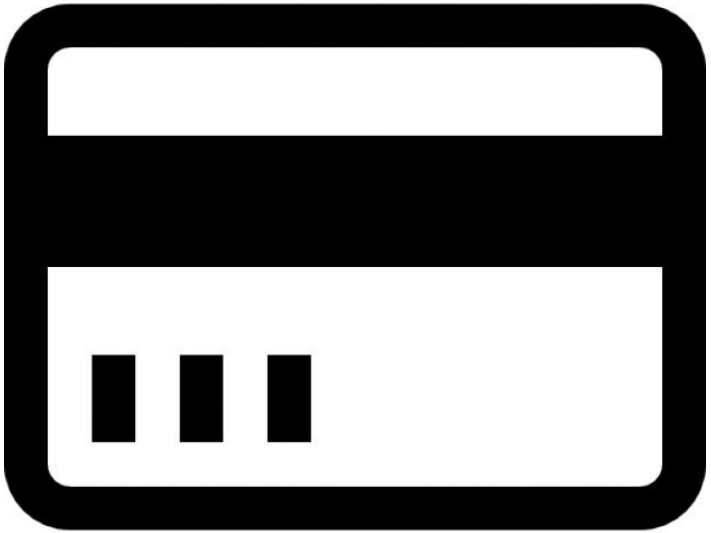
- Например, вы установили на свой андроид некую бесплатную программу с GooglePlay, а вместе с ней к вам на смартфон проник вирус. Номер вашего телефона привязан к карте, т.е. на ваш телефон подключена услуга мобильный банк. Так вот, установленный невзначай вами троянец, может с помощью команд смс-банкинга узнать ваш баланс, отправить смс-команду на перевод с вашей карты на другую, и самостоятельно ответить смс-кой на сообщение о подтверждении операции. Причём владелец смартфона никаких признаков активности может и не увидеть, вирус просто скроет их от него, или увидит, но будет поздно.

Банкомат-фантом

- Вместо настоящего банкомата мошенники могут соорудить пластиковый каркас со встроенным в него скиммером. Со вставленной карты в картоприёмник может считаться вся необходимая информация для её последующего обналичивания и заодно злоумышленники узнают ваш пин-код, набранный на «псевдо-клавиатуре». Как вариант, банкомат может вообще заглотить и не отдать карту.



Скотч-метод



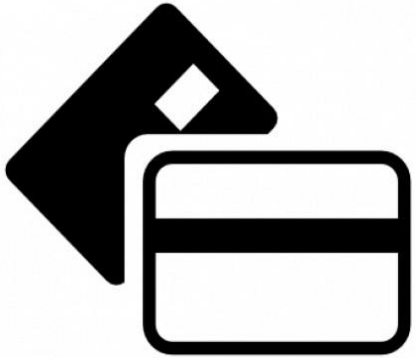
Человек подходит к банкомату, желая снять деньги со своей карточки, вставляет карту в картоприёмник и набирает на клавиатуре пин-код. Со стороны диспенсера слышится характерный шелест, но денег почему-то не видно. Человек «списывает» это на неисправность банкомата, пожимает плечами, вынимает свою карту и идёт к другому банкомату. Что в итоге? Деньги действительно снялись с карточки и даже банкомат их выдал, но они в реальности приклеились к двухстороннему скотчу, прилепленному в диспенсере мошенником, который и вынет деньги за вас.

Письма и звонки от мошенников

Типичный пример смс-мошенничества – это получение смс-сообщения от якобы номера банка о блокировке средств на вашей карточке из-за попытки несанкционированного доступа к ним, с рекомендацией позвонить на номер, приведённый в этом сообщении. По телефону вам сообщат, что для разблокировки денег на счёте карточки необходимо передать её реквизиты: номер карты, ФИО, срок действия и секретный код из трёх цифр на обратной стороне пластика (CVV/CVC).

Письма и звонки от мошенников

Таким образом, незадачливый держатель карточки, чтобы спасти свои деньги, передаёт все важные данные – ему не дают времени на раздумывание и анализ ситуации, в чём и заключается расчёт хитрых злоумышленников. Более того, мошенники ещё и попросят продиктовать им пароль, который пришёл на сотовый телефон жертвы (а это и есть тот самый одноразовый пароль, которым им надо подтвердить операцию перевода денег с атакуемой карты). Если человек не слепой, то в пришедшей смс-ке он увидит фразу о недопустимости передаче одноразового пароля постороннему лицу. Но он это прочитает уже потом, когда поймёт, что с его карточного счёта увели приличную сумму.



Фишинг

Весьма распространённый вид мошенничества, когда, например, пользователю интернета «подсовывают» псевдосайт его интернет-банка, сильно похожий на оригинал, на котором всякими способами будут пытаться выудить (выловить) его карточные данные. Отсюда и название этого способа мошенничества, в переводе с англ. «fishing» – это рыбалка. Главное, чтобы человек перешёл на подставной сайт и поверил, что он находится на оригинальном ресурсе. Ссылку на такие подставные сайты может содержать, к примеру, электронное письмо от мошенника, выполненное в типовой банковской форме (расцветка, логотип и пр.), а текст будет стимулировать по ней перейти, пугая возможными проблемами с деньгами на ваших карточных счетах. При этом названия таких сайтов внешне похожи, но всё же незначительно отличаются. Найдите, например, отличия оригинального названия сайта sberbank.ru от псевдосайта sbepbank.ru. Различия заметить не так просто «неопытному» глазу.

Скимминг

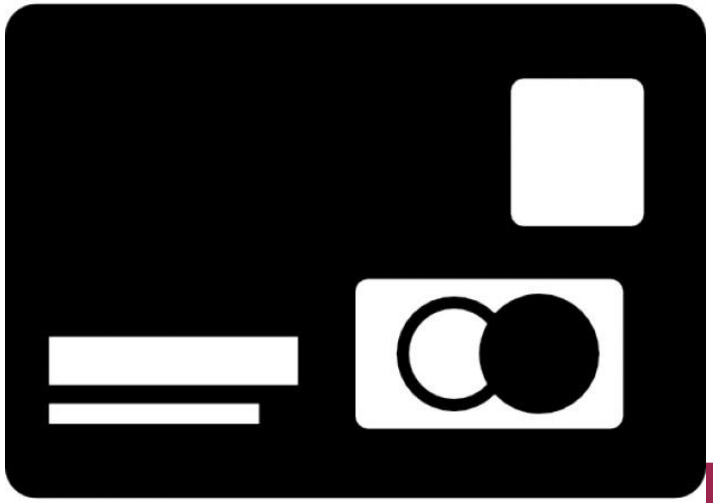
Злоумышленники используют для кражи данных специальные устройства – скиммеры, которые незаметно крепятся к картоприёмнику банкомата и копируют данные с магнитной полосы карточки, когда карта вставляется в слот картоприёмника. Банкомат с прилепленным скиммером неспециалисту трудно отличить от оригинального оборудования – тот же рельеф и цвет. В арсенал мошенников входит накладная клавиатура или миниатюрная камера, необходимые для того, чтобы считать/подглядеть вводимый пин-код. Скопированные данные «заливаются» на карту-болванку, с которой с помощью подсмотренного пин-кода снимается с карты любая сумма.

Признаки установки скимминга

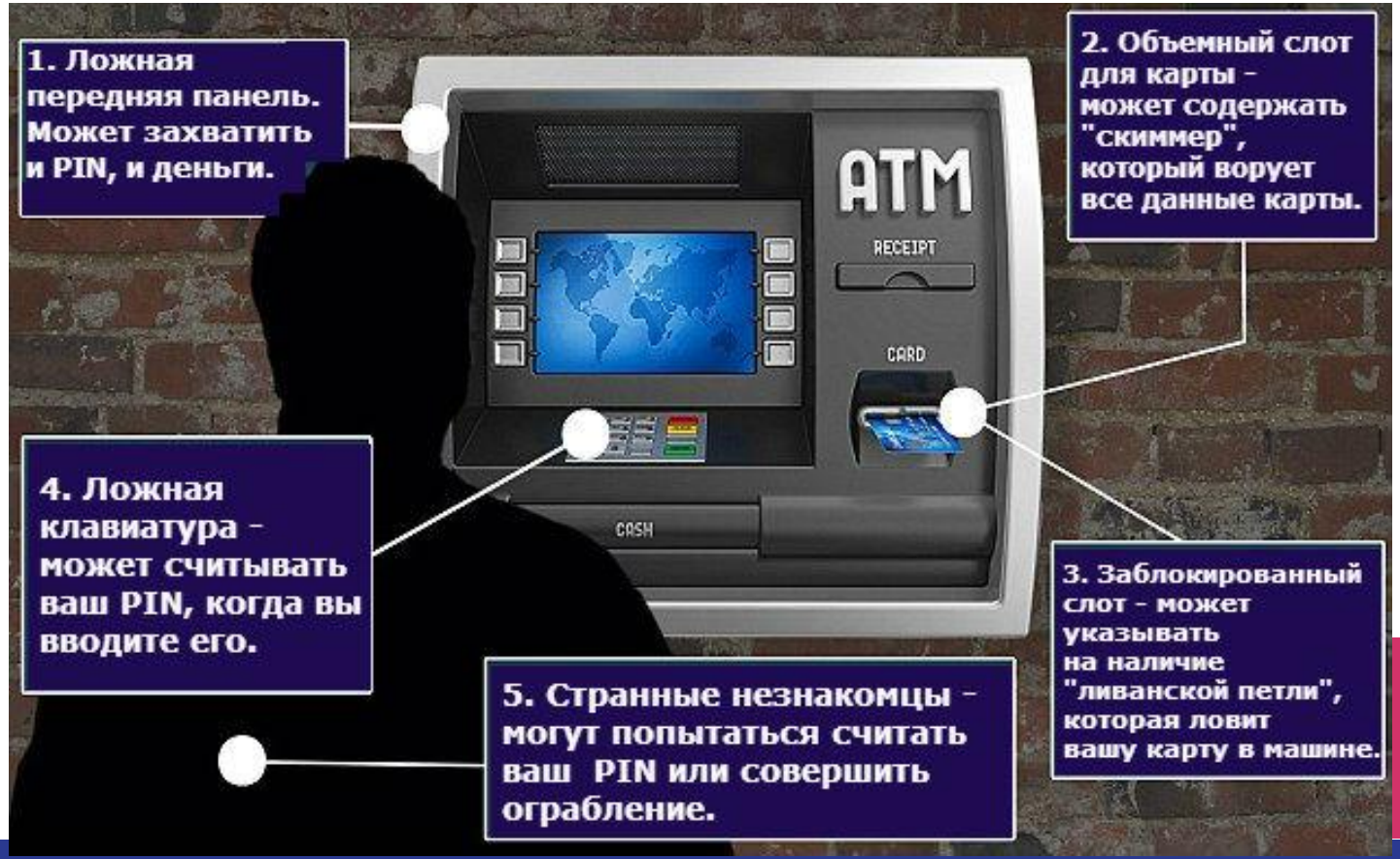
- Непонятные накладки на картоприемнике, некачественно установленные панели или рекламные блоки, маленькие отверстия или неплотно прилегающие детали аппарата. Эти признаки могут указывать на наличие камеры или скиммера.
- Цвет и фактура клавиатуры, имеющие отличия от общего вида устройства указывают на возможную установку считывающей накладки.
- Терминалы, расположенные в неприметных местах, в темном помещении или на проходной улице. Там преступникам проще всего пользоваться своими инструментами.
- Правильным решением будет выбор банкомата в отделении банка или терминала, оснащенного антискимминнговой защитой и физическим барьером против записи ПИН-кода

Ложные устройства

- 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.

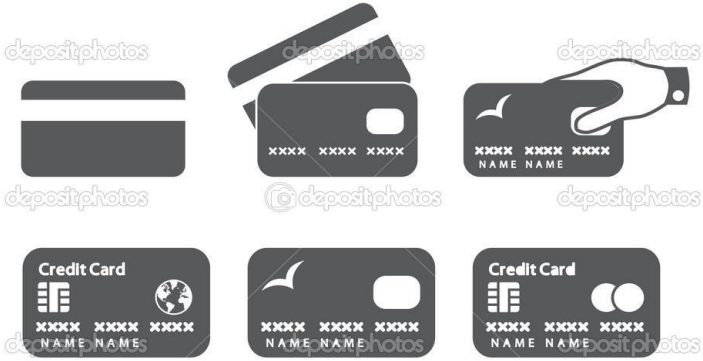


Ложные устройства



Действия после мошенничества

- Если совершено мошенничество с вашей банковской картой, незамедлительно пишите заявление в полицию. При этом можно сразу приобщить к заявлению копию выписки по счету, полученную заранее в банке, где будет видно движение денежных средств по счету. Также можно предоставить детализацию телефонных звонков и смс, если хищение денежных средств произошло путем телефонной связи.



Источники информации

- http://www.banki.ru/wikibank/bankovskaya_karta/
- http://kreditonliner.ru/info_bankkarti_platsystems
- https://ru.wikipedia.org/wiki/Мошенничество
- http://www.sberbank.ru/ru/person/dist_services/warning/cards
- http://creditexpert.su/publication/400-skimming-chto-eto-i-kak-ot-nego-zashchititsya
- http://www.plus-bank.ru/about/pressroom/abc_client/bankovskie-karty/desyat-sposobov-moshennichestva-s-bankovskoy-karto/
- http://www.sberbank.ru/ru/person/dist_services/warning/examples
- http://www.sberbank.ru/ru/person/dist_services/warning/sms-email-secure