МБУК РОСТОВСКАЯ-НА-ДОНУ ГОРОДСКАЯ ЦБС
ЧИТАЛЬНЫЙ ЗАЛ ЦГБ ИМ. М. ГОРЬКОГО

Безопасность при пользовании банковской картой

2018 г.

По данным Банка России, доля несанкционированных снятий средств с "пластиковых" счетов в общем объеме операций, совершенных с использованием платежных карт, в 2017 – 2018 г.г. составила 0,0016 процента. Цифра кажется мизерной лишь на первый взгляд. В абсолютном значении это почти миллиард - 961,3 миллиона рублей. Отрадно, что объем потерь на 10,6 процента меньше, чем годом ранее. Это результат действий Банка России, правоохранительных органов и, конечно, самих операторов по переводу денежных средств.

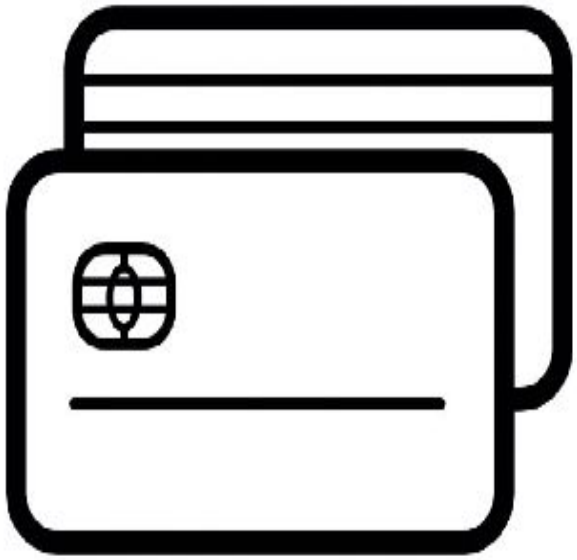
Ба́нковская ка́рта (англ. Bank Card, BCard, BC) - пластиковая карта, привязанная к одному или нескольким расчётным счетам в банке. Используется для оплаты товаров и услуг, в том числе через Интернет, а также снятия наличных.

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

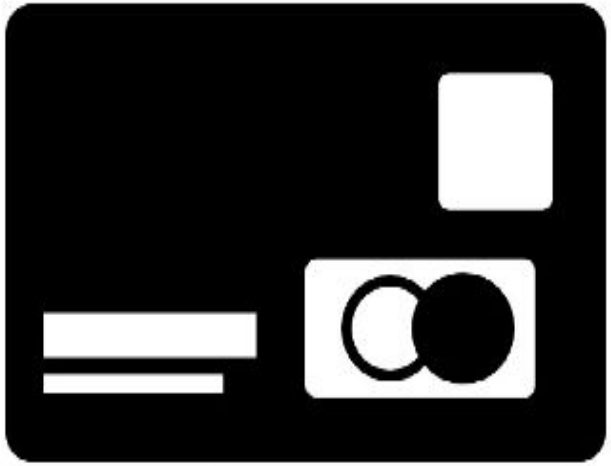
Правила безопасного пользования банковской картой

- 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

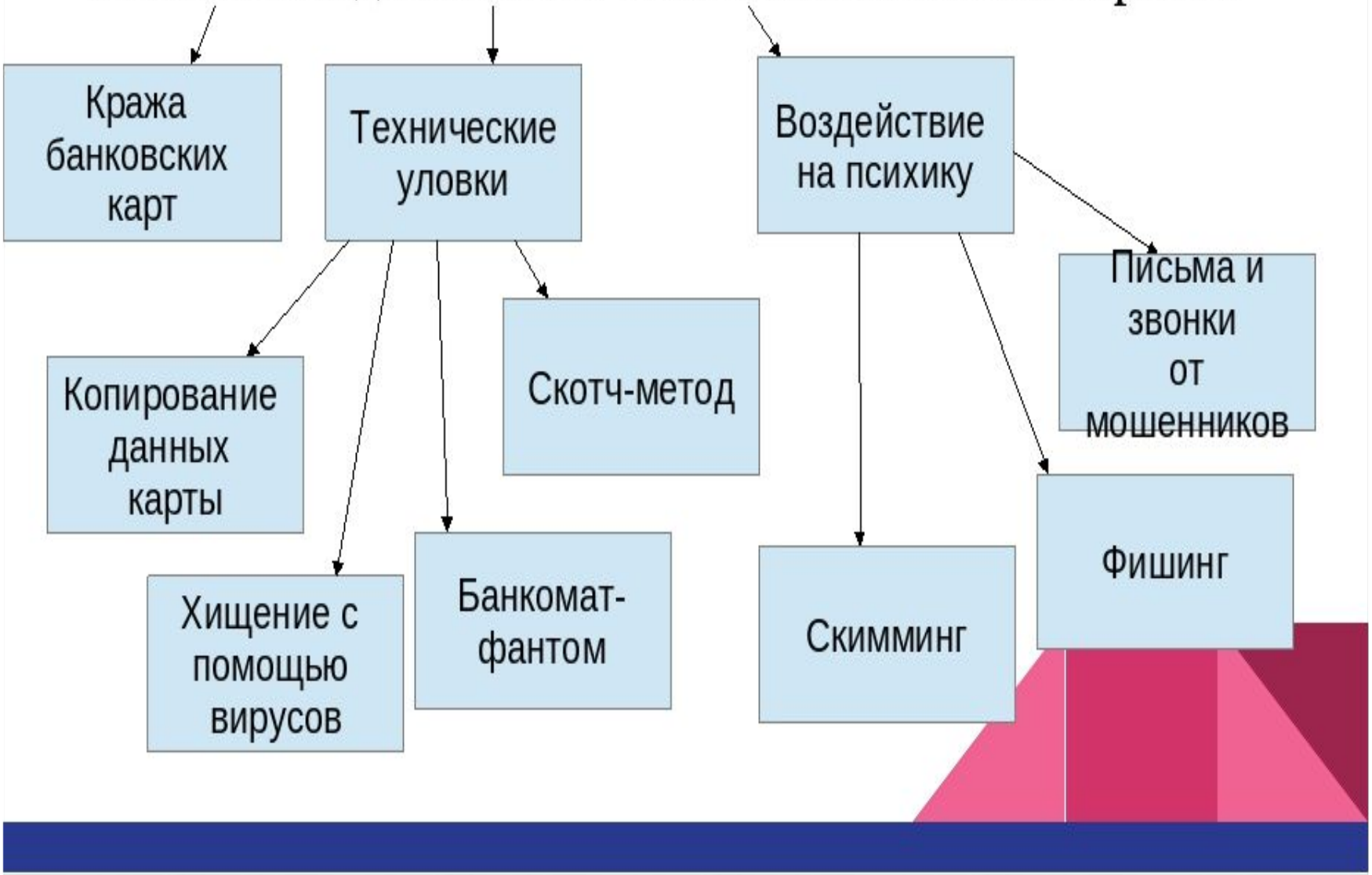


Мошенничество

- 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

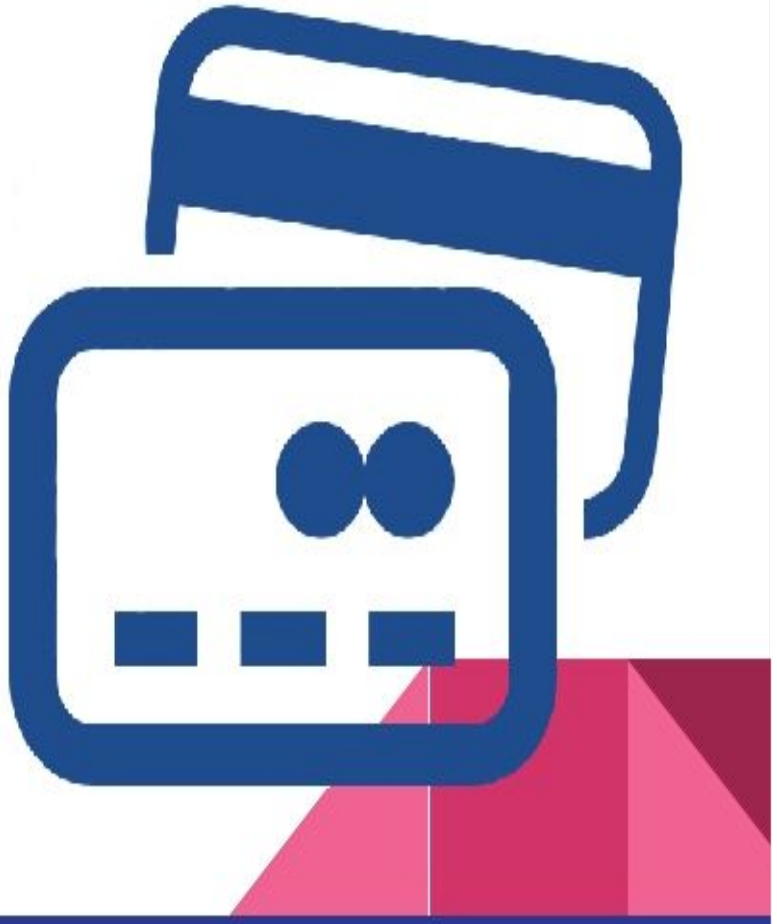


Кража банковских карт

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.

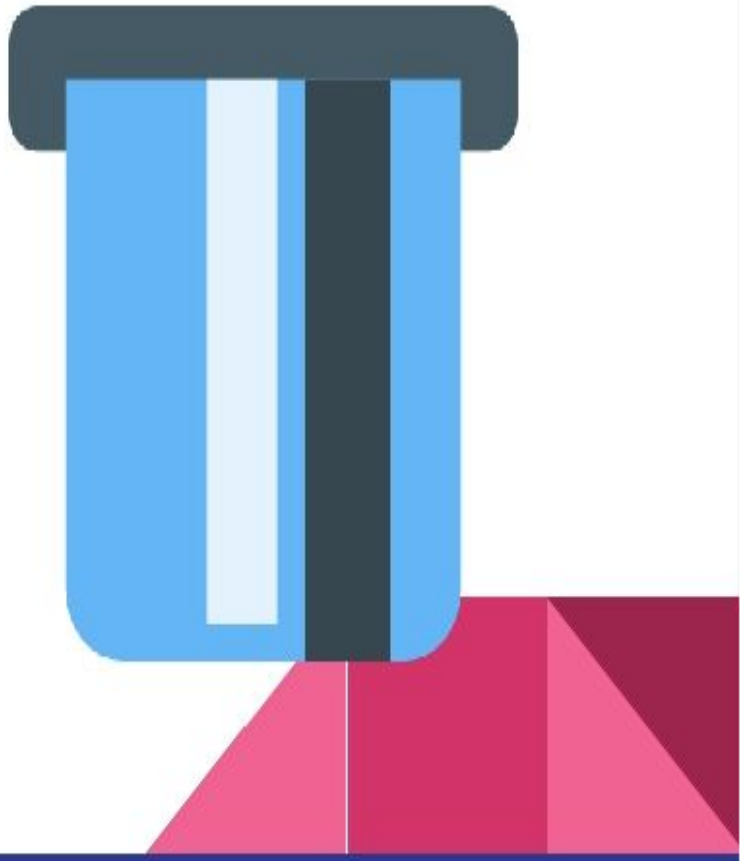
Технические уловки.
Копирование данных карты работниками сферы обслуживания

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.



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.



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).

Скимминг

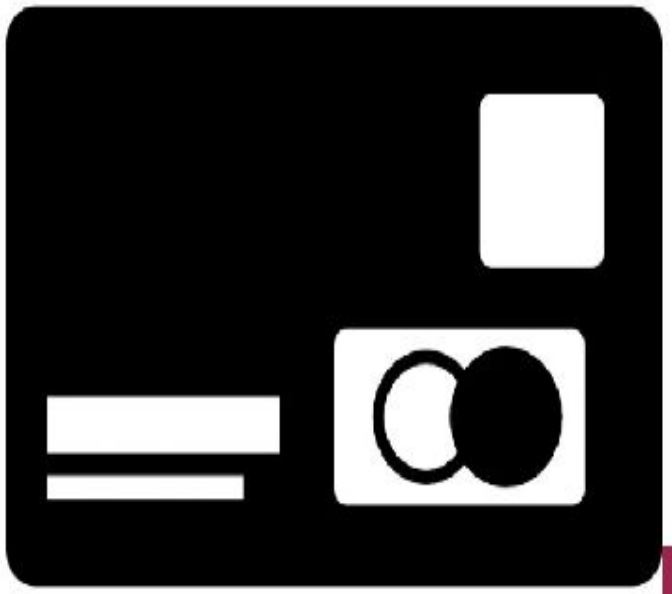
Злоумышленники используют для кражи данных специальные устройства – скиммеры, которые незаметно крепятся к картоприёмнику банкомата и копируют данные с магнитной полосы карточки, когда карта вставляется в слот картоприёмника. Банкомат с прилепленным скиммером неспециалисту трудно отличить от оригинального 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.



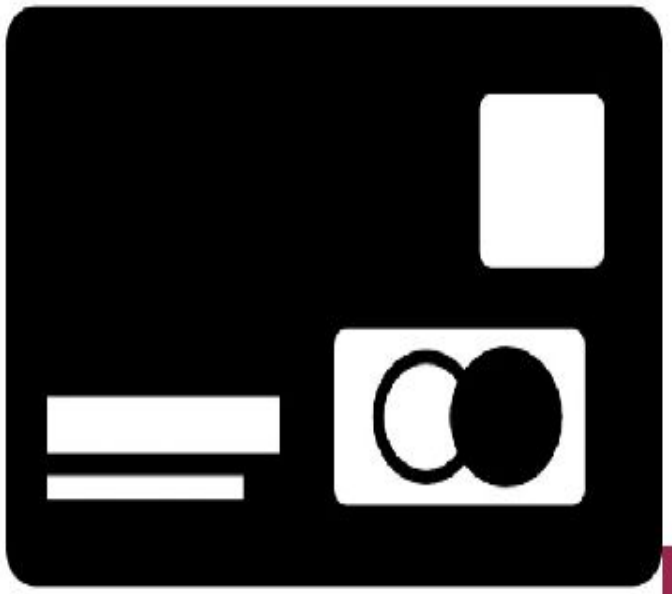
Лукавый расчет

Деньги с банковской карты могут похитить даже там, где вы никак этого не ожидаете. Кассир, официант, заправщик, работник банка или любой другой сотрудник, которому гражданин передал платежную карту для расчета, может сфотографировать, переписать ее данные или просто запомнить их, чтобы потом изготовить дубликат карты. Сделать это можно незаметно. Заранее включается записывающее устройство (это может быть и обычная камера видеонаблюдения), на записи с которого карта видна с обеих сторон. В этом случае мошенникам остается лишь отмотать запись на нужное время и переписать данные карты.

Чтобы этого не случилось, не стоит передавать карту посторонним, рассчитываясь за покупку или предоставление услуг. Обратите внимание на поведение сотрудника, совершающего операцию. Если он фотографирует вашу карту на мобильный телефон под видом набора номера или смс, следует прервать операцию, потребовать возврата карты. И лучше всего обратиться в банк, выдавший карту, с заявлением о ее перевыпуске: ведь вы не знаете, какие данные успел заснять мошенник.

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.



Сам себе взломщик

Нередко мошенники для кражи денег с карты пользуются психологическими приемами для управления действиями человека. Они изображают покупателей щенков, автомобилей, земельных участков, гаражей и т.д. на сайтах бесплатных объявлений или в социальных сетях. Общее у таких "покупателей" одно: они находятся где-то далеко, но для того, чтобы вожделенный товар не приобрел кто-то другой, они готовы перевести часть стоимости или даже полную стоимость немедленно на банковскую карту продавца.

"Покупатель" просит продавца сообщить ему данные карты (код CVV2/CVC2, срок действия, ФИО владельца), чтобы зачислить на нее деньги. Если доверчивый продавец сообщает эту информацию, с его карты начинают списываться деньги за оплату товаров и услуг, осуществляться переводы на другие счета и пр. В некоторых случаях злоумышленник пытается узнать код из смс, который приходит на мобильный телефон. Это значит, что мошенники уже сумели узнать данные карты и не хватает только кода подтверждения транзакции. Получив его, преступники похищают денежные средства.

В этом случае защитить владельца карты может простая осторожность. Не сообщайте данные карты, персональные данные и коды, присланные в смс, посторонним лицам. Не давайте никому доступ к вашей карте через онлайн-банкинг. В любых подозрительных ситуациях нужно звонить в банк, выдавший карту, по номеру, указанному на ее оборотной стороне.

40 процентов мошеннических операций совершается за пределами России, это серьезно затрудняет поиск аферистов

Как минимизировать возможный ущерб? Получив внезапное оповещение об изменении состояния счета после звонков с неизвестных номеров, необходимо немедленно блокировать все свои платежные карты, "привязанные" к этому телефонному номеру. Для этого нужно позвонить на "горячие линии" банков, номера которых указаны на самих картах. Затем обратитесь к мобильному оператору для разблокировки своей сим-карты и одновременной блокировки дубликата, полученного мошенниками. Подайте заявление в правоохранительные органы, даже если мошенники не успели списать средства с ваших карт.

Спасибо

за

внимание!