БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ БАНКОВСКИХ КАРТ

Что следует предпринять, если потеряешь банковскую карту?

Утеря платёжной карты - это самый распространённый риск для ее владельца. Но это не повод для беспокойства о сохранности денежных средств. В этом случае человеку просто необходимо незамедлительно связаться с банком, выпустившим карту, и заблокировать ее. Сделать это можно так: обратиться в службу поддержки клиентов банка по телефону либо направить сообщение для блокировки карты через «Мобильный банк», если такая услуга подключена. Телефон, по которому нужно звонить в экстренных случаях, напечатан на оборотной стороне платёжной карты.

Рекомендуем вам заранее переписать реквизиты карты и контактные данные банка. Всегда держите их при себе, чтобы была возможность связаться с банком в непредвиденных обстоятельствах. Но никогда не переписывайте ПИН-код и не держите его в кошельке вместе с картой, к которой он привязан.

После блокировки потерянной карты вам нужно будет обратиться в банк с письменным заявлением о ее перевыпуске.

Таким же образом следует поступать в случае, если карта заблокирована банкоматом.

Как данные карты могут стать известны мошенникам?

Одной из причин попадания данных карты к мошенникам является неаккуратное обращение с картами самих владельцев, например записанный прямо на карте ПИН - код, проговаривание его вслух при наборе, ввод персональных данных в Интернете на сторонних сайтах и прочее. Нередко преступники прибегают к психологическим уловкам. Так, мошенники могут прислать СМС-сообщение, обратиться к вам по электронной почте, либо по телефону с просьбой уточнить данные вашей карты, банковского счета.

Кроме того, известны такие способы мошеннических действий с банковскими картами как скимминг и фишинг.

Скимминг - изготовление фальшивых платежных карточек и копирование информации с магнитной полосы одной карты на другую. Для этих целей используется скиммер - портативный сканер, считывающий данные с карты жертвы. Выглядит это устройство как накладка, которая устанавливается на отверстие для приема карты. После копирования информации с карты, мошенники изготавливают дубликат карты. Но чтобы воспользоваться такой картой, необходимо знать ПИН-код. ПИН-код считывается при

помощи видеокамеры, установленной неподалеку, либо с помощью накладной клавиатуры, установленной на клавиатуру банкомата.

Фишинг - вид интернет-мошенничества, целью которого является получение доступа к логинам и паролям пользователя. Вот, к примеру, типичный вариант фишинг-атаки: преступники создают подложный сайт кредитной организации или платежной системы, который выглядит «как настоящий». Мошенники пытаются обманным путем добиться от пользователя, посетившего этот сайт, чтобы он ввел свои данные и данные своей карты. Обычно для привлечения пользователей на подложный сайт используется массовая рассылка электронных сообщений якобы от имени действующего банка или иной финансовой организации. Ссылки, содержащиеся в таком письме, ведут на подложный сайт.

Как поступать, если приходит сообщение на телефон, что с карты списана определенная сумма, но владелец карты не совершал покупок?

Самое главное: если в сообщении указан номер телефона, ни в коем случае не перезванивайте по этому номеру. Главная цель мошенников в таком случае – добиться, чтобы жертва вышла на прямой разговор. Мошенники пытаются убедить человека в необходимости сообщить данные карты либо совершить некие действия с картой через банкомат якобы для отмены операции или проверки остатка на карте. Выполнение таких действий приведет к перечислению денежных средств с карты жертвы на счета или электронные кошельки злоумышленников.

Сначала следует убедиться, действительно ли средства с карты были списаны. Для этого надо связаться с банком, который выпустил вам карту, - позвоните по телефону, который указан на оборотной стороне карты. Если карты с собой нет, узнать номер телефона службы поддержки клиентов можно в сети Интернет. Как правило, номер указан на главной странице сайта банка.

Если специалист службы поддержки не подтверждает факт списания средств с карты, скорее всего это сообщение из разряда массово рассылаемых мошенниками для того, чтобы убедить жертву позвонить по указанному в нем номеру телефона. В случае, если хотите иметь подтверждение, что средства списаны не были, можно запросить выписку по счёту карты в ближайшем банкомате или отделении банка.

Банк подтверждает списание? Значит, у кого-то есть доступ к данным вашей карты. В таком случае необходимо заблокировать карту. Для более оперативной связи с банком рекомендуем всегда иметь при себе записанный номер телефона службы клиентской поддержки банка, а также сохранённое СМС-сообщение с текстом-командой для

блокирования карты. Перечислять не нужно: списание денег с баланса карты ещё не означает списания со счета. Списание средств со счета по операциям с картами происходит после получения банком подтверждающих документов. Поэтому клиенту необходимо как можно скорее направить банку уведомление (порядок совершения данной процедуры можно уточнить по телефону службы поддержки) об отмене операции, которую он не совершал. Сделать это надо не позднее дня, следующего за днём получения сообщения о списании. Затем в офисе банка надо написать заявление на перевыпуск карты с указанием подробной информации о происшедшем.

Гражданину, ставшему жертвой мошеннических действий с платёжной картой, необходимо обратиться в правоохранительные органы с заявлением о случившемся, а информацию о факте обращения также необходимо передать в свой банк. Ведь для того, чтобы успешно бороться с преступниками в финансовой сфере, органам правопорядка, как минимум, необходимо иметь информацию о совершении преступлений. В случае если списания не произошло, рекомендуем также обратиться в правоохранительные органы.

Что делать, если владелец карты получает сообщение, что карта заблокирована, и сообщение подписано ЦБ?

Банк России осуществляет свою деятельность в соответствии с Федеральным законом № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)». В соответствии с этим законом Банк России не имеет права осуществлять операции с физическими лицами. Кроме того, Банк России не имеет данных о номерах телефонов клиентов кредитных организаций, не владеет данными о статусах платёжных карт граждан и не осуществляет СМС-рассылку информации.

Если вы получили такое сообщение, можно быть уверенным, что оно направлено мошенниками. В таком случае, если человеку необходимо убедиться, что с картой все в порядке, следует обратиться в банк, выпустивший карту. Затем рекомендуем обратиться в правоохранительные органы. Даже если вы не поддались на уговоры мошенников, не отреагировали на сообщение и не пострадали от их действий, следует обратиться в полицию. Это поможет в расследовании схожих преступлений и предотвратит их в дальнейшем.

По телефону сообщили, что Центробанк должен выплатить мне компенсацию. Но сначала нужно оплатить налог, перечислив его на карту юриста. Как поступить?

Напомню вам, Банк России не осуществляет операции с физическими лицами и не выплачивает какие-либо денежные средства гражданам. Кроме того, Налоговым кодексом

РФ определён перечень налогов, взимаемых в Российской Федерации с физических лиц. Налоги перечисляются в бюджет в соответствии с реквизитами, указываемыми на платёжных документах. Эти документы формируются налоговыми органами без участия юристов, и такие платежи никогда не перечисляются на банковские карты физических лиц.

Страховые выплаты физическим лицам банков, у которых отозвана лицензия на осуществление банковских операций, в соответствии с Федеральным законом осуществляет ГК «Агентство по страхованию вкладов» либо уполномоченные банки – агенты.

Если вы все-таки сомневаетесь, обратитесь в подразделение Банка России, расположенное в вашем регионе письменно или по телефону. Информация о контактах территориальных учреждений есть на официальном сайте Банка России. Можно обратиться непосредственно в интернет-приёмную Банка России через сайт www.cbr.ru. Также каждый желающий может позвонить в контактный центр Банка России на бесплатный номер 8 800 250 40 72 из любого региона России.

Как сделать покупку в интернет-магазине при помощи банковской карты безопасно?

Для безопасности персональных данных и информации о карте лучше всего совершать покупки со своего компьютера, на котором обязательно должна быть установлена антивирусная программа. Для покупок в интернет-магазинах желательно завести дополнительную карту и вносить на неё лишь сумму, необходимую для оплаты предстоящей покупки, или держать постоянно небольшую сумму. Некоторые банки предоставляют возможность использования реквизитов так называемой «виртуальной карты» для оплаты товаров и услуг в интернете. При совершении таких операций не забывайте, что логотип платёжной системы должен соответствовать тому, что указан на вашей карте.

Если вы используете основную банковскую карту, то лучше совершать оплату покупок через сайты тех компаний, которым вы доверяете, а также через сайты, отмеченные значком в виде закрытого замочка или ключика. Помните: при оплате через интернет ни в коем случае не вводите на сайтах ПИН-код карты. Для онлайн-оплаты предназначен CVV-код, указанный на обратной стороне карты. Обычно банками для дополнительной защиты интернет-платежей используются специальные одноразовые коды-пароли, направляемые в СМС-сообщениях. Ни в коем случае не сообщайте данные

своей карты, если вам позвонил представитель торговой фирмы, банка, гостиницы, другой организации, либо вы получили соответствующее письмо по электронной почте.

Как безопасно расплачиваться картой в магазинах, в ресторанах, в кафе?

При оплате картой первое правило: не используйте карту в тех организациях, которые не вызывают у вас доверия. Особенно помните об этом в зарубежных поездках. Всегда требуйте проведения операции в своём присутствии, не выпускайте ее из вида. Это необходимо для снижения риска неправомерного получения ваших персональных данных, указанных на карте. В кафе и ресторане требуйте переносной терминал, чтобы провести оплату лично. Если вам в этом отказывают - пройдите к кассе вместе с официантом или расплатитесь наличными.

При совершении оплаты товаров и услуг с использованием карты кассир может попросить у вас предоставить паспорт, подписать чек или ввести ПИН-код. Вводя ПИН-код, убедитесь, что его не могут увидеть люди, находящиеся в непосредственной близости. Перед тем, как подписать чек, обязательно проверьте сумму, указанную в нем. При совершении операции за границей обращайте внимание на валюту совершаемой операции и действуйте исходя из того, какова валюта счета вашей карты во избежание дополнительных конвертаций.

Иногда операция по оплате картой не одобряется с первого раза. Что делать в таком случае?

Если не одобряется операция по карте, которую вы проводите в переносном терминале, причин может быть несколько: сбой связи, ошибка при вводе ПИН-кода или недостаточность средств на карте. В таком случае списания с карты, как правило, не происходит. Попробуйте ввести ПИН-код ещё раз. При этом сохраните чек с информацией о том, что операция не может быть произведена, и постарайтесь в кратчайшее время проверить баланс карты в ближайшем банкомате или отделении банка во избежание двойного списания. Можно также обратиться по телефону в службу поддержки банка. В этом случае помните, что сотруднику службы поддержки для подтверждения вашей личности могут потребоваться данные вашей карты, паспорта и кодовое слово, указанное вами при оформлении договора на выпуск карты. Но ПИН-код вы сообщать не должны даже в этом случае.

Что можно сделать, чтобы риск потери от действий мошенников свести к минимуму?

Чтобы свести потери от мошенников к минимуму, необходимо соблюдать простые правила обращения с платёжными картами, а именно:

- не позволяйте никому использовать вашу карту;

- никогда и никому (даже родственникам) не сообщайте ПИН-код. Помните: операция, совершенная с вводом ПИН-кода признается выполненной держателем карты;

- если не можете запомнить ПИН-код и записываете его, то держите его отдельно от карты. Никогда не записывайте ПИН-код на карте;

- никогда не передавайте карту для использования другим людям. Давая карту для оплаты, следите, чтобы кассир совершал операции у вас на глазах, перед вводом ПИН-кода проконтролируйте сумму операции на чеке;

- вводя ПИН-код, прикрывайте свободной рукой клавиатуру, следите, чтобы рядом не было посторонних «наблюдателей». При совершении операции через банкомат не прибегайте к помощи либо советам третьих лиц, свяжитесь со своим банком – он обязан предоставить консультационные услуги по работе с картой;

- перед тем, как воспользоваться банкоматом, обратите внимание на устройство на предмет наличия на нем дополнительных устройств, накладок на клавиатуру или прорезь для приёма карт. Если возникают сомнения – откажитесь от использования такого банкомата. Не используйте неисправный банкомат;

- для оплаты через Интернет используйте одноразовую «виртуальную карту» или заведите дополнительную карту. Перечисляйте на неё денежные средства под расчёт предполагаемой операции;

- используйте на своём компьютере антивирусное программное обеспечение и не открывайте почтовые сообщения с исполняемыми файлами. Лучше вообще не открывать подозрительные сообщения, отправленные с незнакомых адресов;

- можно воспользоваться услугами, которые предлагают банки: можно установить суточный/месячный лимит на совершение операций, блокировку операций по территориальному признаку, заблокировать отдельные услуги;

- учитывая, что в большинстве случаев жертвы сами сообщают данные своих карт мошенникам, будьте бдительны, не сообщайте эту информацию третьим лицам, чем бы они не объясняли такую необходимость.

Кроме того, не забывайте, что сейчас операции переводу денежных средств или по оплате товаров и услуг можно совершать с использованием устройств мобильной связи: телефонов, смартфонов, - это так называемый «мобильный банкинг». В данном случае для минимизации рисков хищения денежных средств следует также бережно обращаться не только с картой, но и с мобильным телефоном. Рекомендуем:

- установить на устройство мобильной связи антивирусное программное обеспечение, базы которого будут регулярно обновляться;

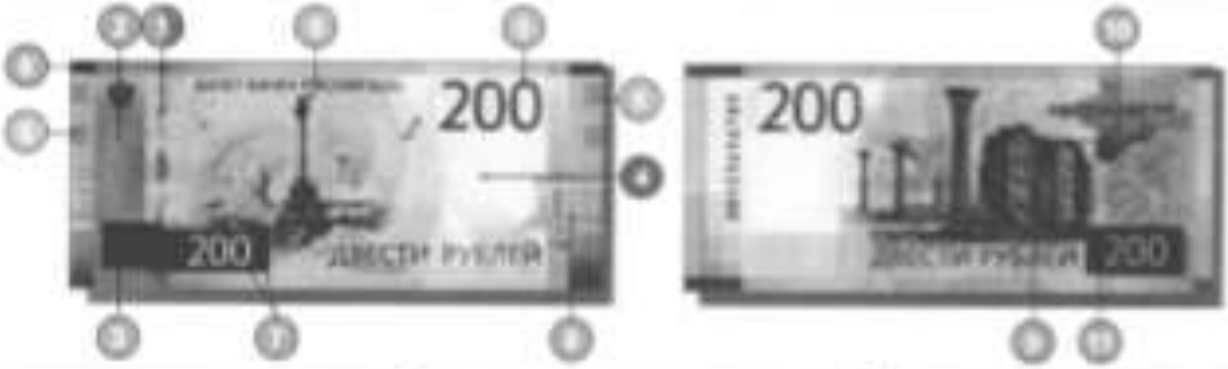
- не передавайте мобильный телефон для использования третьим лицам;

- если вы сменили номер телефона мобильной связи, обязательно сообщите об этом в свою кредитную организацию.

В случае утери мобильного телефона нужно незамедлительно заблокировать карты, которые привязаны к вашему «мобильному банку».

200 РУБЛЕЙ
ОБРАЗЦА 2017 ГОДА

Банк России



ПРИ НАКЛОНЕ

При повороте банкноты от себя либо на противоположную защитную ленту, расходящуюся на поверхность банкноты, наблюдается перемещение блестящих горизонтальных элементов вверх и вниз противоположных направлениях друг относительно друга. Под остальными углами наблюдения визуализируется цветное изображение символа рубля на радужном фоне.

На одной стороне при при изменении угла зрения становится видимым число «200», каждая цифра которого имеет свою окраску. При повороте банкноты на 180° была изменена угла зрения скрытого каждая цифры меняется.

При изменении угла зрения становится видимым символ рубля, который в зависимости от расположения банкноты выглядит темным на светлом фоне или светлым на темном фоне.

НА ПРОСВЕТ

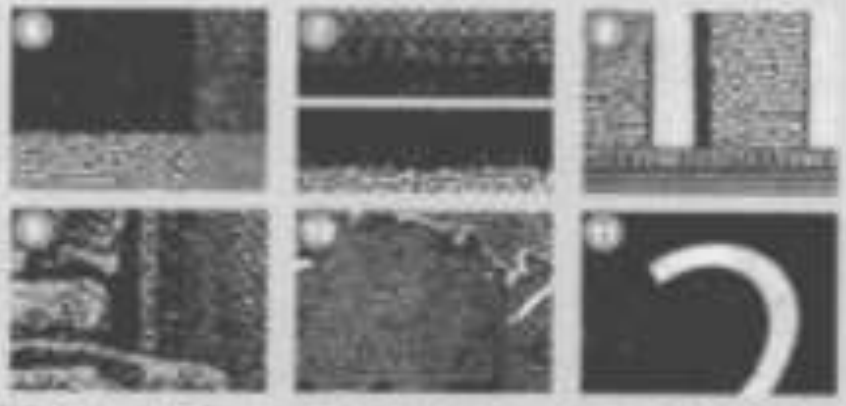
Защитная лента имеет вид темной полосы со светлым повторяющимся числом «200».

Многоцветное изображение водяной знак выполнено в отличие изображения от светлых участков с темным в сочетании с контрастными цветными участками.

НА ОЩУПЬ

Текст «Билет Банка России» строки по краям банкноты и число «200» имеют специальный рельеф.

ПРИ УВЕЛИЧЕНИИ



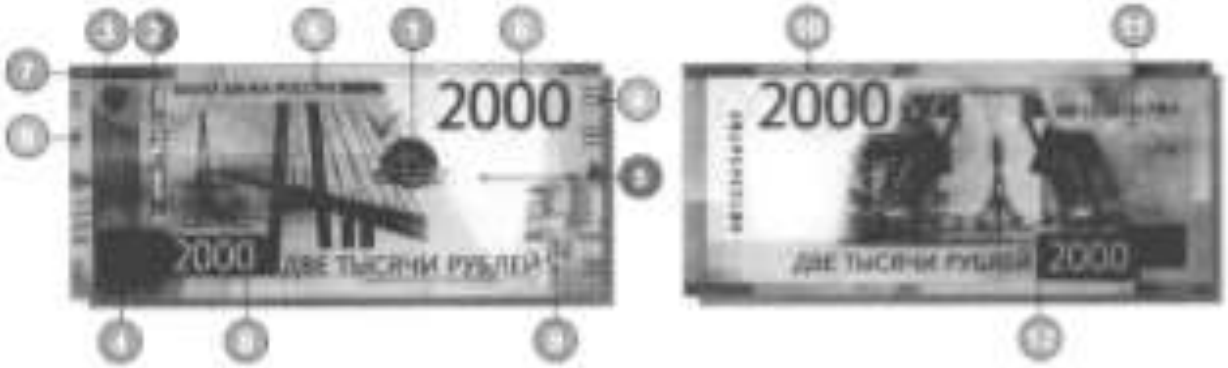
Часть фрагментов изображения содержит мелкие графические элементы, которые надписи, элементы изображения представляют буквы и фразы, которые трудно

Банк России напоминает, что для надежного определения подлинности банкноты необходимо проверить не менее трех защитных признаков.

Информацию об образцах и признаках подлинности денежных знаков Банка России размещена на официальном сайте Банка России

2000 РУБЛЕЙ
ОБРАЗЦА 2017 ГОДА

Банк России



ПРИ НАКЛОНЕ

При наклоне банкноты на изображении герба цифра меняется перемещающимся пучком блестящих полос.

При повороте банкноты от себя или на защитной ленте наблюдается движение изумрудно-цифр номинала исчезающего вдоль относительно друг. Под острым углом наблюдения металлизированное изображение цветных изображения номинала рубля на радужном фоне. По изображения номинала рубля наблюдается состояние между изображением номинала.

На одностороннем поле при изменении угла зрения становится видимым число «2000», каждая цифра которого имеет свой оттенок. При повороте банкноты на 180° (без изменения угла зрения) порядок каждой цифры меняется.

При изменении угла зрения становится видимым самое рубля сегодня в зависимости от расположения банкноты выглядит темным на светлом фоне или светлым на темном фоне.

НА ПРОСВЕТ

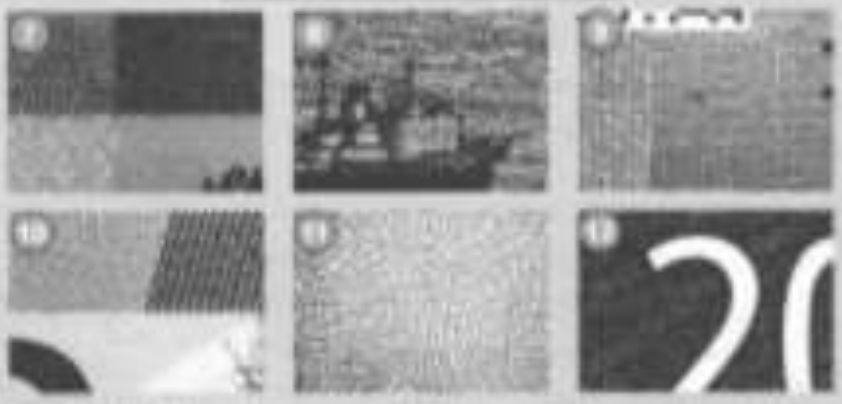
Защитная нить имеет вид темной полосы со светлой повторяющейся аббревиатурой «ЦБ РФ».

Многоцветный комбинированный водяной знак выполнен с плавным переходом от светлых участков к темным и включает в контрастными светлыми участками.

НА ОЩУПЬ

Текст «Билет Банка России», штрихи по краям банкноты и число «2000» имеют повышенный рельеф.

ПРИ УВЕЛИЧЕНИИ



Часть элементов изображения содержит малые графические элементы, включая надписи, орнаменты, изображения представляющие буквы и фигуры (дополнительно).

Банк России напоминает, что для надежного определения подлинности банкнот необходимо проверить не менее трех защитных элементов.

Информация об оформлении и признаках подлинности денежных знаков Банка России размещена на официальном сайте Банка России http://www.cbr.ru