

## **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 наклейка, 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, которые выглядят «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. Нервничать 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 преступлениями 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](http://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