

Как не стать жертвой мошенников и сохранить деньги на банковской карте

Советы для граждан по защите банковских сбережений на картах

С 01.01.2014 года вступило в силу положение статьи 9 Федерального закона от 27 июня 2011 г. №161-ФЗ «О национальной платежной системе», обязывающее банк возместить суммы, перечисленные со счета клиента в результате не санкционированной им операции, если только не будет доказано нарушение данным клиентом порядка использования электронного средства платежа (например, передача данных третьим лицам или их небрежное хранение).

Подключите в банке услугу SMS-оповещений, чтобы быть в курсе всех операций по карте. Если кто-то попытается воспользоваться вашим счетом, вы сразу узнаете об этом в SMS-оповещении и успеете заблокировать карту. Если карта при вас, а в SMS-оповещениях приходит информация о списании средств – срочно звоните в банк, блокируйте карту и просите принять заявление о спорной транзакции (операции). Если карту украли – надо написать ещё и заявление в полицию.

Не оставляйте свои номера телефонов и тем более данные карт и счетов на сомнительных информационных ресурсах. Совершать платежи по Интернету возможно только на тех сайтах, где адресная строка начинается с символов https, где «s»- сигнал о том, что передача данных ведется по безопасным каналам. Если символ «s» адресной строке отсутствует, это знак того, что ваши сведения могут быть украдены.

К своей банковской пластиковой карте необходимо относиться, как кошельку - бережно и держать подальше. Не передавать третьим лицам. Не стоит записывать ПИН-код и хранить его рядом с картой. Желательно ПИН-код запомнить. Держите под рукой номера круглосуточной службы поддержки банка. Не звоните по номеру, который пришел в SMS!

Если вам пришло SMS якобы из банка с просьбой перезвонить по указанному номеру или набрать комбинацию цифр, не делайте этого. Проверьте информацию и состояние своего счета через службу поддержки своего банка и следуйте инструкциям. Всегда имейте при себе номера круглосуточной службы поддержки банка, чтобы иметь возможность проконсультироваться в подозрительных ситуациях.

Помните, что, если вы не используете SIM-карту в течение длительного времени, оператор вправе перепродать номер другому абоненту. А если к этому номеру была привязана ваша банковская карта, то его новый владелец сможет получить доступ и к вашему счету. Передавая карту работникам заведений, в которых вы расплачиваетесь, не выпускайте ее из виду. Оплата должна происходить открыто.

При возникновении проблем во время работы с банкоматом (например, застряла карта) никуда не отходите от банкомата, не обращайтесь к посторонним, а срочно звоните в банк для разрешения возникшей ситуации.

Не переводите деньги с вашей карты в интернет-магазины, посмотрите отзывы об этом ресурсе на других сайтах. Для дистанционной оплаты желательно использовать не «зарплатную» карту, а специально открытый для этих целей карточный счет с ограниченной суммой средств.

Желательно пользоваться банкоматом, расположение которого указывается в официальной информации. Необходимо обращать внимание на внешний вид банкомата. Если что-то вызывает подозрение, найдите другой банкомат.



Сфотографируйте памятку себе на телефон