Простые правила, которые помогут сохранить деньги на карточке в целости и сохранности

Не храните ПИН-код рядом с картой и не пишите его на самой карте.

Прикрывайте рукой клавиатуру, когда вводите пин-код от карты на банкомате. Убедитесь, что ваши действия никто не видит.

Помните о безопасности в интернете: не устанавливайте нелицензионные приложения, не заходите на подозрительные сайты. При установке банковских приложений убедитесь, что их разработчик – ваш банк, а не стороннее лицо. И не забывайте обновлять антивирусную систему.

Не доверяйте СМС с сообщениями о блокировке карты, не переходите по ссылкам из смс-сообщений или мессенджеров. Возникли сомнения? Позвоните в банк по номеру, который указан на вашей карте.

Не давайте свою карту никому в руки.

Если вы сменили номер или потеряли сим-карту, первым делом позвоните в банк и «отвяжите» старый телефон от банковской карты.

Что делать, если вы пострадали от действий мошенников

Срочно позвонить в свой банк

Например, в Сбербанке действует бесплатная круглосуточная «горячая» линия. Набирайте 900 с мобильного телефона (звонок на территории России бесплатный).
Номер 8 800 555-55-50 - для бесплатных звонков с любых телефонов на территории России и +7 495 500-55-50 - для звонков из любой точки мира (стоимость звонка по тарифам оператора связи).

Приготовьтесь сообщить информацию, по которой вас смогут идентифицировать.

Вам потребуется назвать фамилию, имя и отчество, паспортные данные и иную информацию по запросу оператора

Попросите зарегистрировать заявление на незаконные действия с вашей картой.

После вашего сообщения о несанкционированных действиях с картой оператор должен немедленно ее заблокировать, даже если были похищены все средства, хранящиеся на ней.

Обратитесь в полицию

Подайте в любое подразделение полиции заявление о совершенном мошенничестве.

ОСТОРОЖНО МОШЕННИКИ!

НЕ ДАЙ СЕБЯ ОБМАНУТЬ!

Будьте бдительны при совершении действий с банковским картами и соблюдайте элементарные правила безопасности, чтобы не стать жертвой мошеннических действий.

БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Вам поступил звонок (сообщение) о блокировке банковской карты или подозрительных операциях с деньгами – это **МОШЕННИК**. Прекратите разговор и позвоните на горячую линию банка.

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ

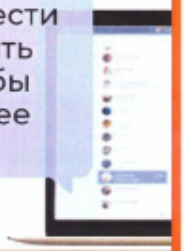
Вам позвонили от имени близкого человека, сообщили о несчастном случае и требуют деньги – это **МОШЕННИК**. Прекратите разговор и позвоните близкому человеку.

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ

По Вашему объявлению о продаже товара в Интернете Вам позвонил покупатель и попросил сообщить реквизиты банковской карты и смс-код, чтобы перевести деньги - это **МОШЕННИК**. Прекратите разговор и ни в коем случае **не сообщайте номер банковской карты и ее код**

СООБЩЕНИЕ В СОЦИАЛЬНОЙ СЕТИ

Ваш друг (родственник) пишет Вам в социальной сети с просьбой срочно перевести в долг деньги или сообщить данные Вашей карты, чтобы перечислить их Вам, скорее всего - это **МОШЕННИК**.



В СЛУЧАЕ ХИЩЕНИЯ ВАШИХ ДЕНЕГ ИЛИ ПРИ ПОДОЗРЕНИИ СОВЕРШЕНИЯ В ОТНОШЕНИИ ВАС МОШЕННИЧЕСКИХ ДЕЙСТВИЙ, НЕМЕДЛЕННО ПОЗВОНИТЕ В ПОЛИЦИЮ ПО ТЕЛЕФОНУ «112».

Мошенники и банковские карты

Кража карт

Схема мошенничества:
1. Мошенник ворует сумку с кошельком, кошелек, либо саму карту
Если в кошельке вместе с картой лежит ПИН-код, то мошенник опустошает карту в ближайшем банкомате
Если ПИН-кода нет, то мошенник делает попытку опустошить карту, покупая высоко ликвидные товары (бытовая и компьютерная техника, ювелирные изделия, мобильные телефоны, банзин, алкоголь и т.д.) в магазинах, принимающих карты, либо интернет-магазинах и сервисах интернет-оплаты банковской картой.

Хранение карт (недопущение хищения)

- Не храните и не оставляйте карты на столах, в шкафах, сервантах, на полках и не разбрасывайте их на видном месте, ни дома, ни на работе
- Не храните карту в кошельке, если носите его в сумке
- Не носите карты вместе с паспортом и другими документами, удостоверяющими вашу личность
- Лучшее место для стационарного хранения карт - сейф или запирающийся ящик стола
- Если вы носите кошелек с деньгами в сумочке, карты лучше хранить в отдельном кармашке сумочки
- Чтобы не забыть карту в магазине, возьмите за правило каждый раз, совершая покупку, проверять куда положили карту.

Мошенники и банковские карты

Фишинг

Цель мошенника проста - узнать логины, пароли, номера карт и кодов CVV2/CVC2 жертвы. Далее, используя полученные данные, мошенники получают доступ к банковским картам, on-line кабинетам интернет-банков и пересылают средства на мошеннические счета или совершают покупки в интернет-магазинах.

Для этого используются разнообразные приемы

1. Мошенник звонит клиенту и представившись сотрудником банка сообщает, что у клиента возникла некая проблема (возможны варианты), для решения которой клиент срочно должен назвать ряд сведений о карте.
2. Жертва получает СМС с сообщением, что его карта заблокирована и номером телефона якобы службы поддержки, звонящих на указанный номер, мошенники "обрабатывают", используя растерянность клиента и в ходе разговора узнают, необходимые для мошенничества данные
3. Мошенник, зная логин и пароль клиента, направляет жертве письмо, что с его карты произошло мошенническое списание средств и для отмены транзакции необходимо назвать код, полученный по СМС от банка. На сомом деле СМС код подтверждает инициированную мошенником операцию и используя названный жертвой код мошенник отправляет средства со счета жертвы на свой счет, либо оплачивает услуги провайдеров.