Владелец банковской карты должен держать этот инструмент в безопасности. Нужно не только хранить карту в надежном месте, но и уберечь ее от мошенников. Если данные вашей карточки попадут в руки преступника, то вы можете потерять ваши деньги, а если карта кредитная, то и получить большой долг.

Как защитить денежные средства на банковской карте от мошенников?

Стоп!

Мошенник!

Фишинг

Этот вид мошенничества заключается в том, чтобы достать реквизиты карты обманным путем:

✓ мошенники создают сайт, который маскируется под интернет-магазин, платежный сервис или даже банк;

✓ мошенник может представиться сотрудником банка, который потребует сообщить реквизиты карточки и PIN-код – например, чтобы разблокировать ее;

✓ если вы разместили объявление о продаже чего-либо в соцсети или на торговой площадке, то злоумышленник позвонит под видом покупателя и попросит сообщить все данные карты, чтобы перевести деньги.

!!! Не оставляйте данные карточек на подозрительных сайтах. Перед покупкой чего-либо в интернет-магазине проверьте его надежность и безопасность – изучите отзывы, свяжитесь с поддержкой, попросите показать документы о регистрации. Подключение к сайту должно быть защищенным: адрес сайта должен начинаться с «https://».

!!! Также не сообщайте никому данные карты по телефону.

SMS

При таком способе мошенничества вы получите на свой телефон сообщение с подозрительным содержанием. Цель у него, как и у фишингового сайта – заставить человека тем или иным способом сообщить мошеннику реквизиты карты.

✓ ваша карта заблокирована. Для разблокировки вам предлагают позвонить по указанному в сообщении телефону. Если вы позвоните по этому номеру, то от вас потребуют сообщить данные карточки;

✓ родственник или ваш ребенок сейчас в тяжелой ситуации и ему срочно требуются деньги. В сообщении указан номер счета, куда требуется отправить нужную сумму. В таком случае мошенник получит и деньги, и данные карты;

✓ вы выиграли в каком-либо розыгрыше призов. Но, чтобы забрать награду, вам нужно отправить некоторую сумму на счет организатора – например, заплатить за доставку.

!!! Никогда не отвечайте на подозрительные SMS.

!!! Также желательно добавить подозрительные номера в черный список вашего телефона. Тогда вы избежите повторных звонков и сообщений.