Финансовая грамотность и безопасность

ВТБ

Основные виды мошенничества с банковскими картами

Скимминг

Мошенники устанавливают на банкомат специальное устройство, считывающее данные банковской карты

Телефонное мошенничество

Звонки и смс-сообщения под разными предлогами, чтобы выманить банковские реквизиты или деньги у жертвы

Хищение данных с помощью вирусов

Рассылка на устройства потенциальных жертв вредоносного ПО

Фишинг

Создание поддельного сайта, имитирующего подлинный, для получения доступа к данным пользователя (логины, пароли и др.)

Мошенничество при покупках в интернете

Мошенник представляется покупателем и, под предлогом перевода денег, узнает реквизиты карты

Слева — банкомат без скиммера, справа — со скиммером

накладная клавиатура

Скрытая видеокамера

РОЦИТ

Как обезопасить свою ***банковскую карту***

ВТБ

1

Не давайте свою банковскую карту никому в руки и старайтесь сохранять ее от лишних глаз

2

Не рассказывайте и не посылайте никому свои банковские реквизиты

3

Не оплачивайте покупки ***с чужих электронных устройств***

4

Если вы часто совершаете покупки в интернет-магазинах, заведите для этих целей ***отдельную банковскую карту***

5

Устанавливайте ***суточные лимиты*** на все виды совершаемых операций по вашей карте

6

Не вводите данные своей карты на ***подозрительных веб-сайтах и ресурсах***

7

Не подтверждайте по смс операции, ***которые вы не совершали***

8

Если видите снятие денег без вашего участия — ***сразу блокируйте карту***

9

Выбирайте банкоматы, которые находятся на территории банков и офисов