

Финансовая  
грамотность  
И  
безопасность



# 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 предложениями, 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**

# Как обезопасить свою банковскую карту

1

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



Не рассказывайте и не посылайте никому свои банковские реквизиты

2



Не оплачивайте покупки с чужих электронных устройств

3



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

4



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

5



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

6



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

7



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

8



**Выбирайте банкоматы**, которые находятся на территории банков и офисов

9

