Банк России

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ БАНКОВСКИХ КАРТ

Сальников А.А. 2019 г.

Бюджет России $15 * 10^{12}$ (15 триллионов)

7 из 10 совершеннолетних россиян имеют банковские карты

Объем операций по картам граждан $100 * 10^{12}$ (100 триллионов)

Объем мошеннических операций по картам $1 * 10^{9}$ (1 миллиард)

Количество мошеннических операций по картам 300 000

Средняя сумма одного хищения 3000


SAMSUNG
pay
pay
Pay


ТРУДОВАЯ
КНИЖКА

Потеря тайны данных, достаточных для платежа:

- ✓ номер карты, ФИО, срок действия, CVV/CVC/CVP

Телефонное мошенничество, методы социальной инженерии:

- ✓ попытка узнать реквизиты карты
- ✓ попытка получить код из смс-подтверждения
- ✓ принуждение к платежу, переводу средств

Банкомат, POS-терминал:

- ✓ перехват реквизитов карты и персональных данных
- ✓ тайна ПИН
- ✓ скиммер, накладной ПИН-пад, ливанская петля
- ✓ хищение карты

Интернет-угрозы, фишинг:

- ✓ сайты-“двойники”
- ✓ интернет-магазины “однодневки”
- ✓ массовые рассылки
- ✓ вредоносные программы

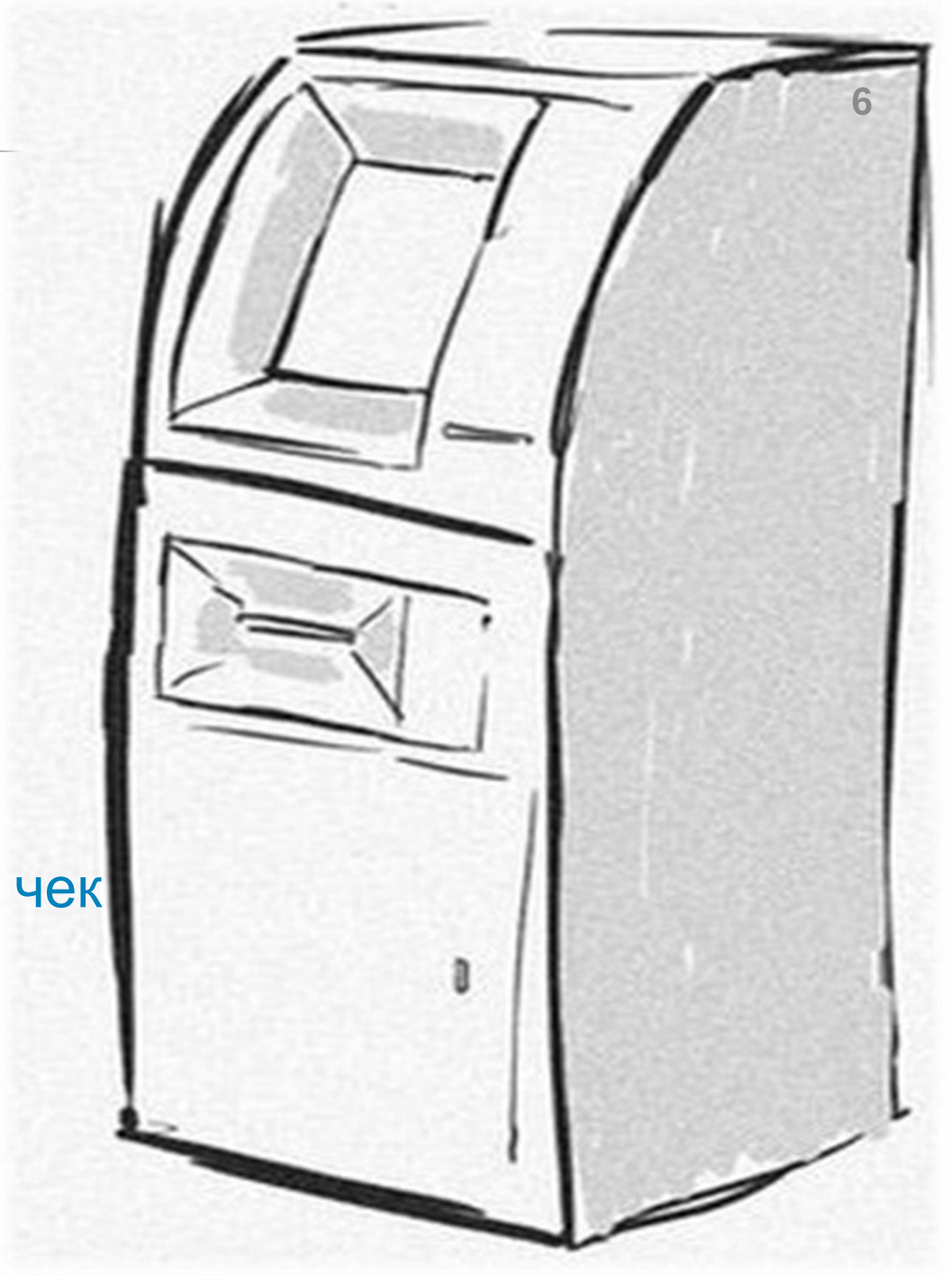
Цель мошенника:

Узнать персональные данные, реквизиты карты или счета, пароли, коды, вызвать на беседу, заставить открыть ссылку на вредоносный ресурс

✓ Возможна подмена телефонного номера звонящего

Ваши действия:
Игнорировать такие звонки и СМС, или задать встречные вопросы: мои ФИО, номер карты, адрес?

- ✓ Небезопасное месторасположение
- ✓ Ввод ПИН для замка двери при входе
- ✓ Наблюдение за вводом ПИН
- ✓ Установленные скиммеры / шиммеры
- ✓ Карта тяжело входит в картоприемник
- ✓ Подозрительные сбои в работе
- ✓ Не пересчитаны полученные деньги
- ✓ Не сохранена или выброшена квитанция, чек
- ✓ Следование советам злоумышленников
- ✓ Невозврат карты
- ✓ Подставной банкомат



Скиммер / Шиммер:

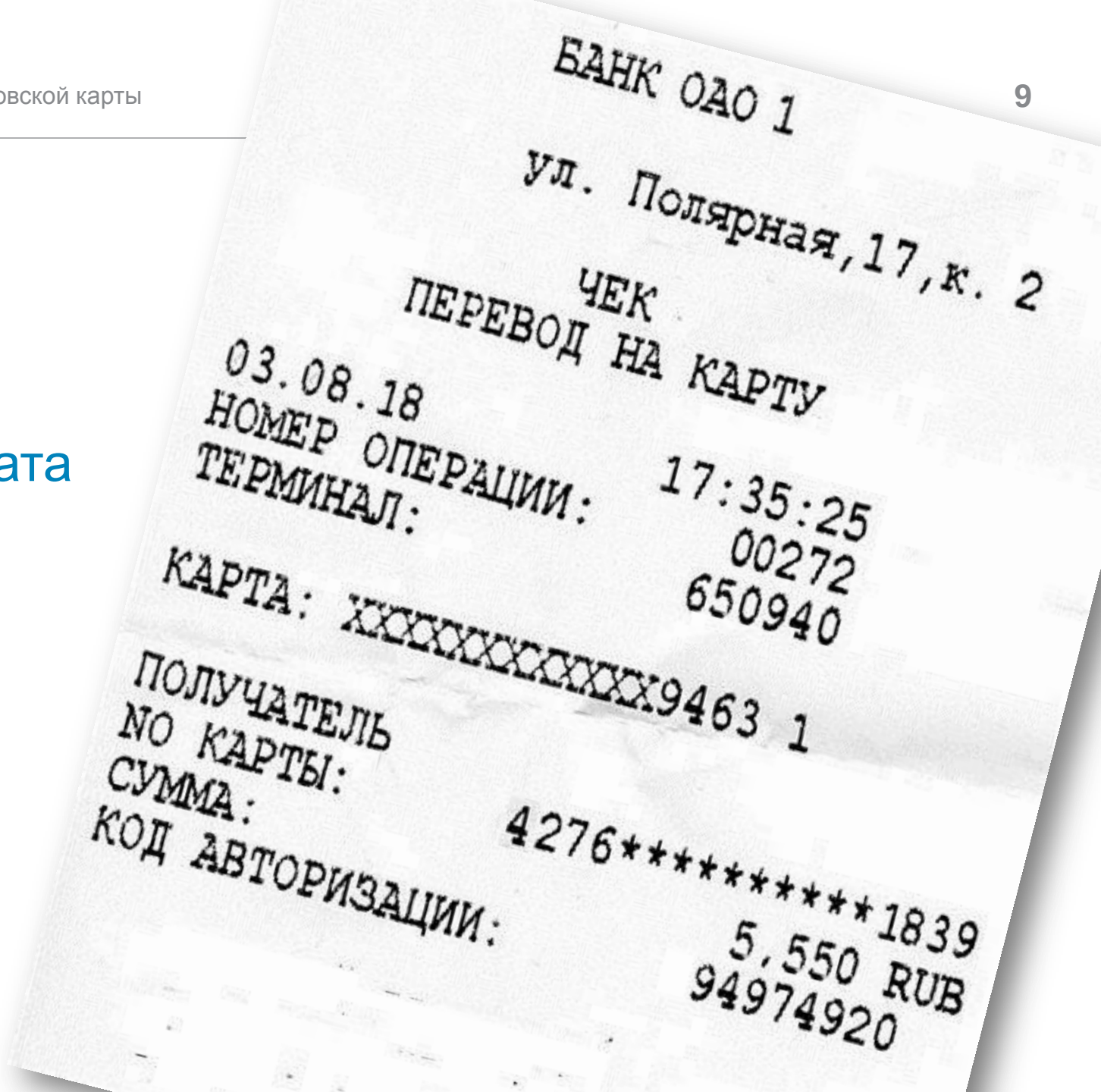
Считывание и передача злоумышленнику кодов и реквизитов карты, достаточных для совершения платежа

Ложный ПИН-пад:

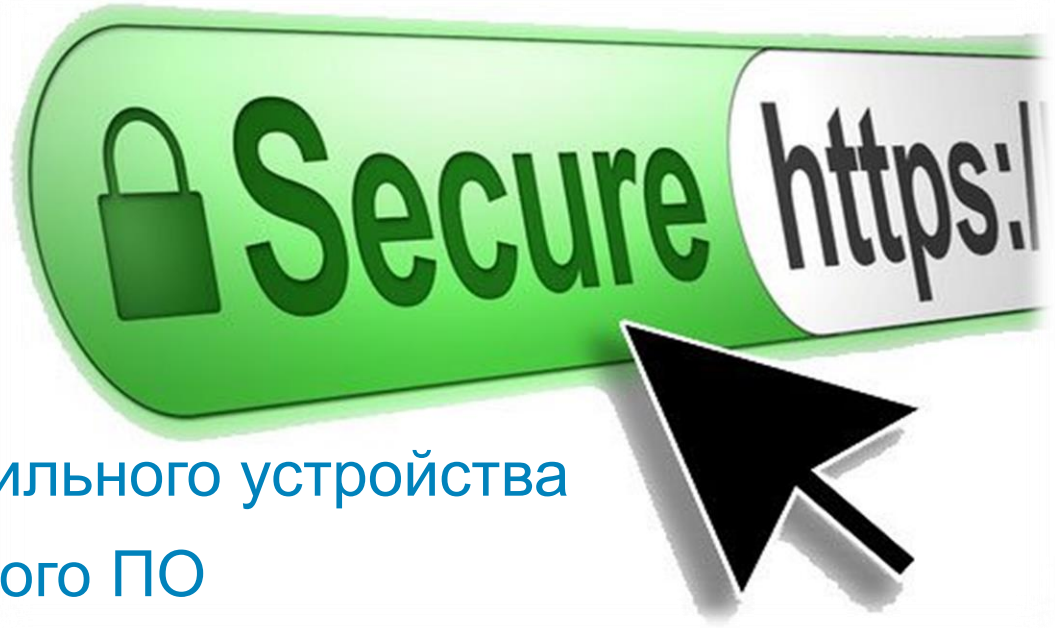
Ввод ПИН не в настоящий ПИН-пад, а в его имитацию, которая передаст злоумышленнику введенный код

- ✓ Недобросовестные организации
- ✓ Передача карты в чужие руки
- ✓ Проведение операции без сверки суммы перед оплатой
- ✓ Наблюдение злоумышленников
- ✓ Не сохранение чека отмененной или не проведенной операции
- ✓ Оплата в два приема для обхода лимита операции без ввода ПИН
- ✓ Непосредственное использование карты с NFC чипом

- ✓ Вид операции
- ✓ Дата и время операции
- ✓ Номер операции
- ✓ Номер терминала / банкомата
- ✓ Реквизиты карты
- ✓ Сумма и валюта операции
- ✓ Код авторизации
- ✓ Размер комиссии
- ✓ Остаток средств
- ✓ Разовые пароли доступа



- ✓ Ввод ПИН
- ✓ Использование постороннего WiFi соединения
- ✓ Незащищенное интернет соединение
- ✓ Использование основной карты
- ✓ Покупки на подозрительных сайтах
- ✓ Покупки на сайтах-“двойниках”
- ✓ Покупки с постороннего компьютера, мобильного устройства
- ✓ Отсутствие средств защиты от вредоносного ПО
- ✓ Отсутствие мер противодействия вредоносному ПО



Банк России

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ БАНКОВСКИХ КАРТ

7 ПРАВИЛ

- Снимайте наличные только в проверенных банкоматах
- Запомните или добавьте телефон банка в контакты
- Запомните и нигде не записывайте ПИН
- Подключите СМС-оповещения и подтверждения
- Не переходите по ссылкам, присланным посторонними
- Используйте для покупок в Интернете отдельную карту
- Делайте онлайн-покупки только на проверенных сайтах

ФИНАНСОВОЕ БЛАГОПОЛУЧИЕ

ФИНАНСОВАЯ ГРАМОТНОСТЬ

Бдительность

Знания

Надежность аппаратуры

Защищенность программ

Банк России

СПАСИБО
ЗА ВНИМАНИЕ

Пункт приема корреспонденции:
Москва, Сандуновский пер., д. 3, стр. 1, телефон +7 495 621-09-61
Почтовый адрес: 107016, Москва, ул. Неглинная, д. 12
Контактный центр: 8 800 250-40-72, +7 495 771-91-00
Факс: +7 495 621-64-65, +7 495 621-62-88
Сайт: www.cbr.ru
Электронная почта: cbr@cbr.ru