«Мошенничество с банковскими картами»

Банкомат-фантом

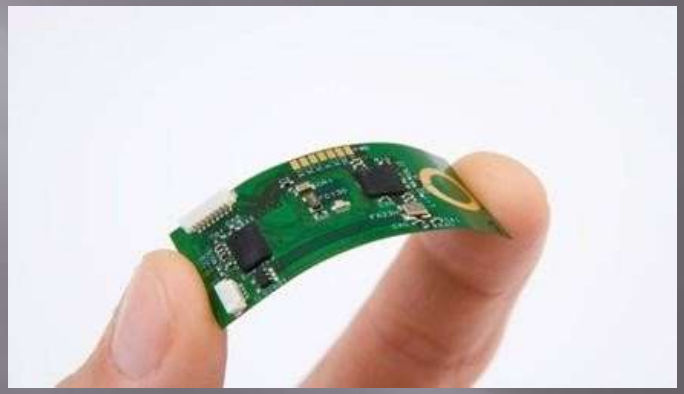
В месте, неконтролируемом службами охраны, устанавливается похожий на настоящий банкомат.

Отличительные особенности:

- **Не подключен к источникам внешнего питания;**
- **Вес значительно ниже настоящего банкомата;**
- **Расположен, как правило, вне помещения.**

Скриминг в банкоматах

Шиммер

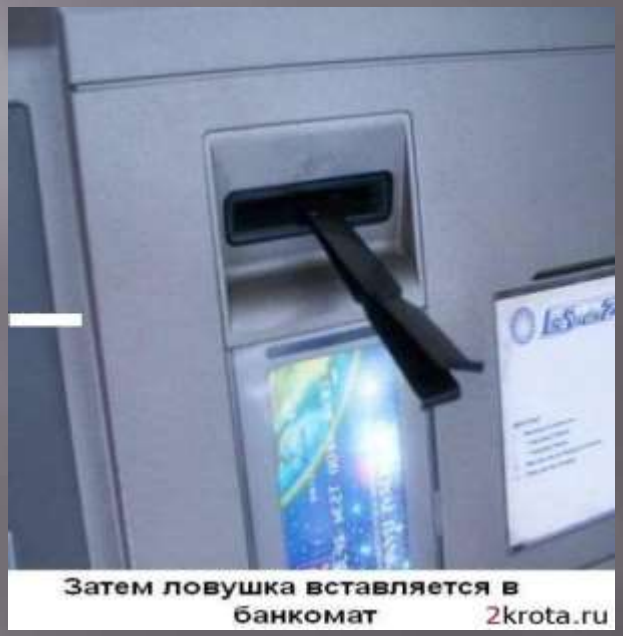


Фальш-накладка для считывания магнитной полосы карты

Накладная клавиатура для считывания ПИН-кода карты

Ливанская петля

Ливанская петля **— это устройство для блокировки картридера (картоприемника) банкомата**



Фишинг

Фишинг - мошенничество с банковскими картами может осуществляться через интернет, телефон

Цель мошенников **— получить идентификационные данные держателя банковской карты:**

- **Номер карты;**
- **Срок окончания действия;**
- **CVC2-код;**
- **Логин;**
- **Пароль.**

Снифферинг

Мошенник использует анализатор трафика, или сниффер (от англ. to sniff — нюхать) — сетевой анализатор трафика, программа, предназначенная для перехвата и последующего анализа, либо только анализа сетевого трафика.

Чехол для защиты банковских карт от несанкционированного считывания секретной информации

Вредоносные программы

Сетевые черви

Компьютерные вирусы

Троянские программы

Кража банковских карт

Схема мошенничества:

1. Мошенник ворует сумку с кошельком, кошелек, либо саму карту

2. Если в кошельке вместе с картой лежит ПИН-код, то мошенник опустошает карту в ближайшем банкомате

Не дай себя обмануть!

Материал подготовили: Кошкарева С.В.
Малышева Е.В