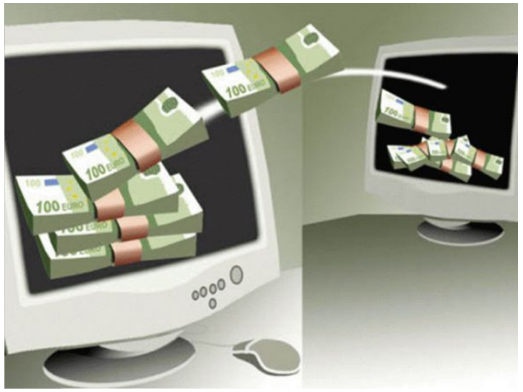


# Финансовое мошенничество и пирамиды: теория, признаки и принципы

# Мошенничество

Статья 159 УК РФ

**Мошенничество**

«хищение чужого имущества или приобретение права на чужое имущества путем обмана или злоупотребления доверием»

**Финансовое мошенничество**

совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

# Статистика ущерба от случаев мошенничества с банковскими картами

| Год | | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|---|---|
| Ущерб (руб.) | Официальные данные МВД | 77,2 млн. | 38,6 млн. | 32,2 млн. | 140 млн. | 150 млн. | 130 млн. |
| | Данные ЦБ | 1,25 млрд. | 1,46 млрд. | 2,7 млрд. | 3,6 млрд. | 4,6 млрд. | 3,5 млрд. |

фишинг

скимминг

нигерийски
е письма

ливанская
петля

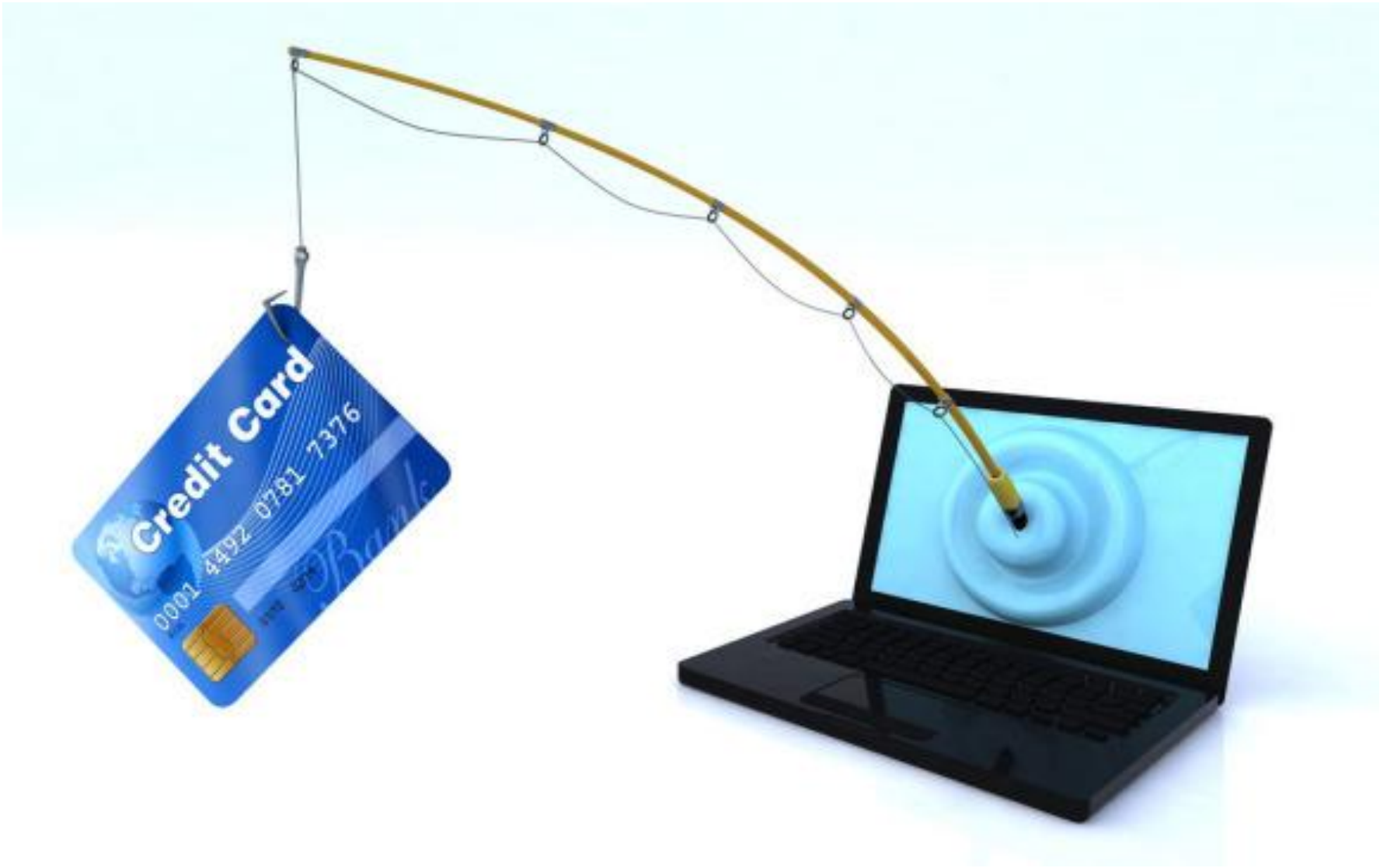
вишинг

фарминг

шиммминг

скотч-
метод

# Фишинг



# Информация, представляющая ценность для фишера:

- фамилия и имя пользователя;
- адрес и номер телефона;
- пароль/пин-код;
- номер дебетовой/кредитной карты;
- CVC/CVV;
- номер социального страхования;
- номер банковского счета.

# CVC/CVV


123
Your CVV
VISA
VISA
ELECTRON
MasterCard
DISCOVER
NETWORK

# Правила защиты от фишинга:

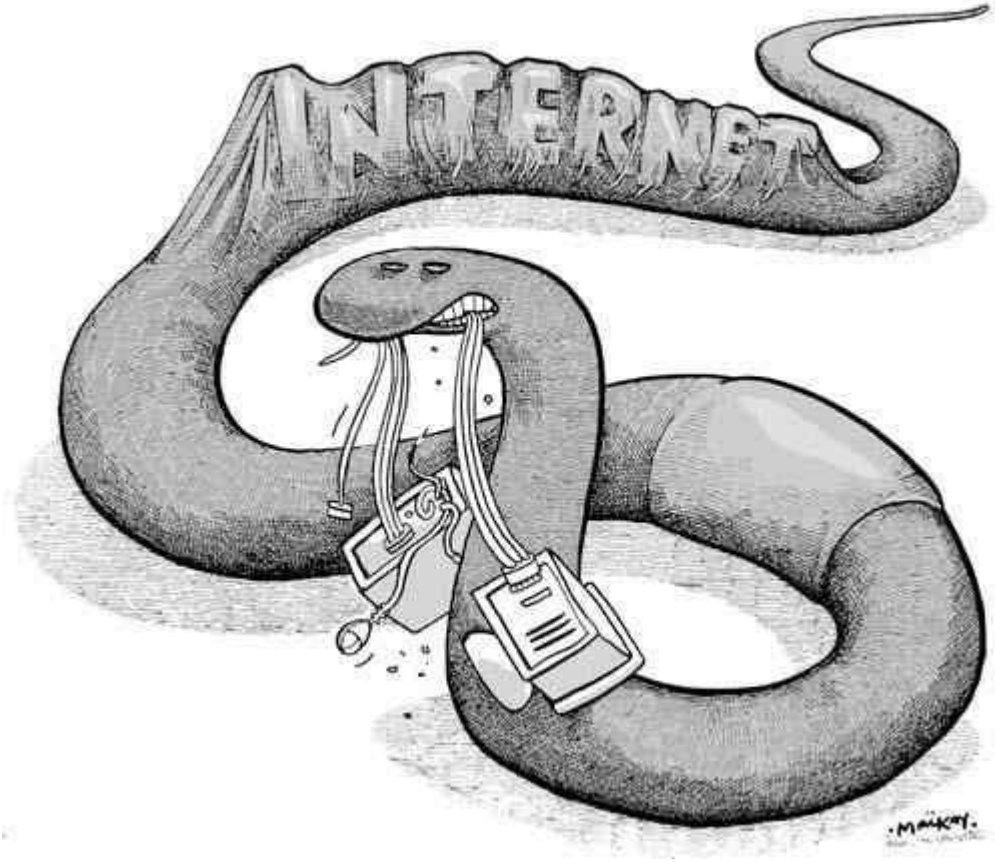
- внимательно проверять доменное имя сайтов, на которых необходимо ввести персональные данные;
- не доверять сообщениям, которые просят внести личные данные, лучше созвониться с банком, если что-то насторожило;
- регулярно обновлять антивирусное ПО, которое отвечает за доступ к сайтам.

# Вишинг

# Правила защиты от вишинга:

- при получении подозрительного звонка, необходимо незамедлительно перезвонить в банк и уточнить ситуацию;
- ни в коем случае нельзя звонить по указанному мошенниками в сообщении номеру и выдавать личную информацию;
- соблюдать осторожность при передаче любых личных данных через интернет, телефон и т.д.;
- регулярно отслеживать состояние своего счета, контролируйте все траты с карты.

# Фарминг



# Вирусы, поражающие банкоматы

# Скимминг

# Примеры скимминговых устройств

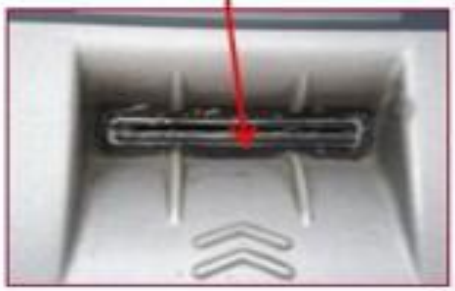
## Пример 1

ФАЛЬШ- НАКЛАДКА ДЛЯ СЧИТЫВАНИЯ МАГНИТНОЙ ПОЛОСЫ КАРТЫ

НАКЛАДНАЯ КЛАВИАТУРА ДЛЯ СЧИТЫВАНИЯ ПИН-КОДА

## Пример 2

БАНКОМАТ НА КОТОРОМ УСТАНОВЛЕНЫ СЧИТЫВАЮЩИЕ УСТРОЙСТВА



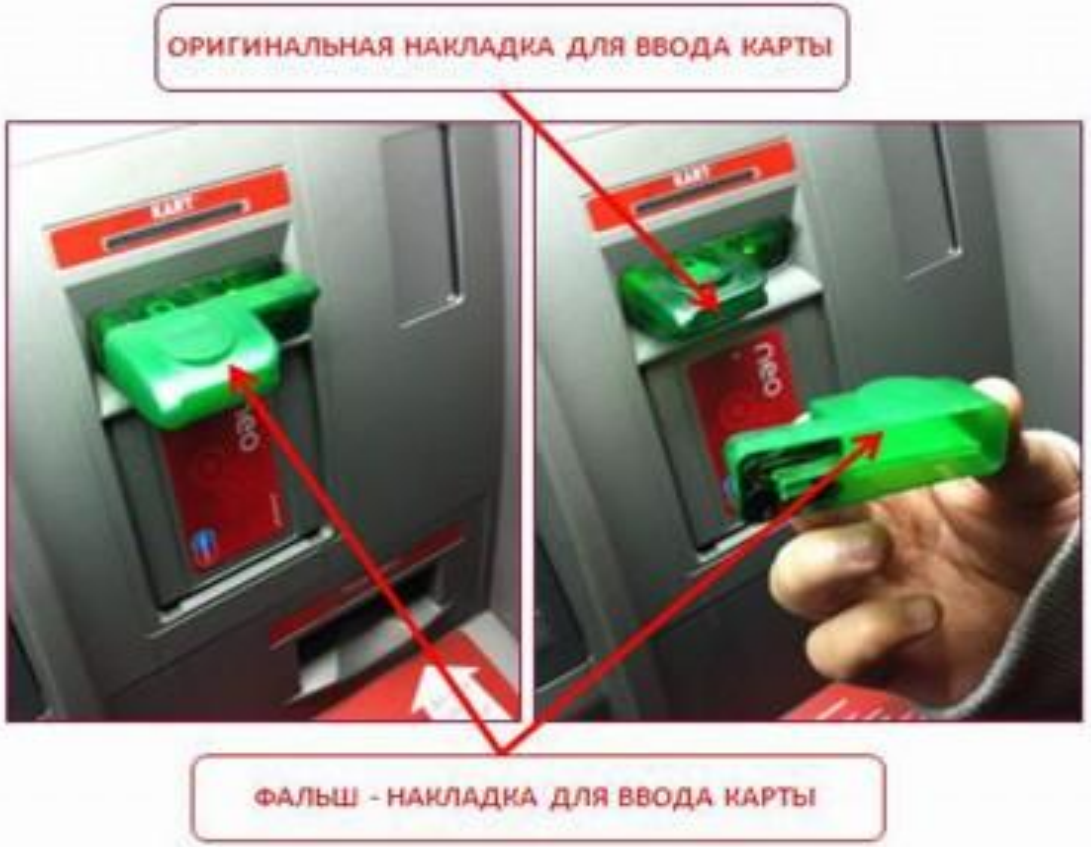
ФАЛЬШ- НАКЛАДКИ ДЛЯ СЧИТЫВАНИЯ МАГНИТНОЙ ПОЛОСЫ КАРТЫ

ВИДЕОНАБЛЮДЕНИЕ ЗА ВВОДОМ ПИН-КОДА

# Примеры скимминговых устройств

Пример 3


Пример 4

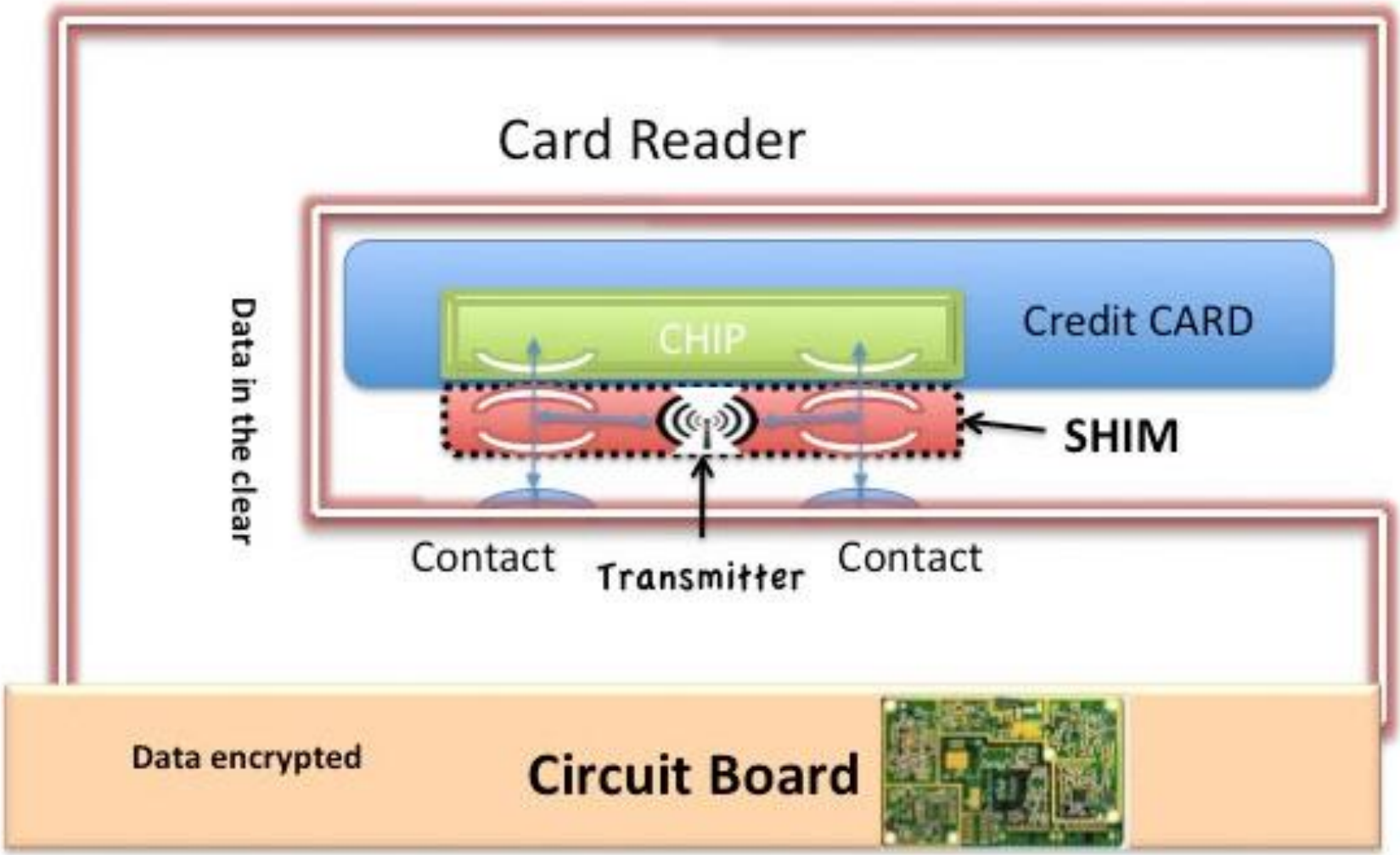


# Правила защиты от скимминга:

- стараться использовать банкоматы, находящиеся вблизи банка. Чем больше будет вблизи такого банкомата камер наблюдения, тем лучше;

- внимательно исследовать банкомат на предмет наличия «странных» конструкций: накладная клавиатура бывает заметна, под ней виден оригинал, а также мини-камера, которая может быть вмонтирована в банкомат.

# Шимминг


Card Reader
Data in the clear
CHIP
Credit CARD
SHIM
Contact
Transmitter
Contact
Data encrypted
Circuit Board

# Ливанская петля

Ловушка делается из материала, используемого для рентгеновских снимков

Затем ловушка вставляется в банкомат

После ухода жертвы престпник достает карточку, потянув за края

# Ливанская петля

# Правила защиты от ливанской петли:

- если банкомат захватил вашу карту, нужно осмотреть щель картоприемника и при обнаружении торчащих из нее посторонних предметов, попробовать их вынуть. Тогда, возможно, карту удастся вернуть самостоятельно;

- прежде чем покинуть банкомат, не вернувший вашу карту, следует заблокировать ее по телефону своего банка и не покидать банкомат до момента подтверждения банковским сотрудником блокировки карты. Впоследствии, карту можно будет разблокировать или перевыпустить;

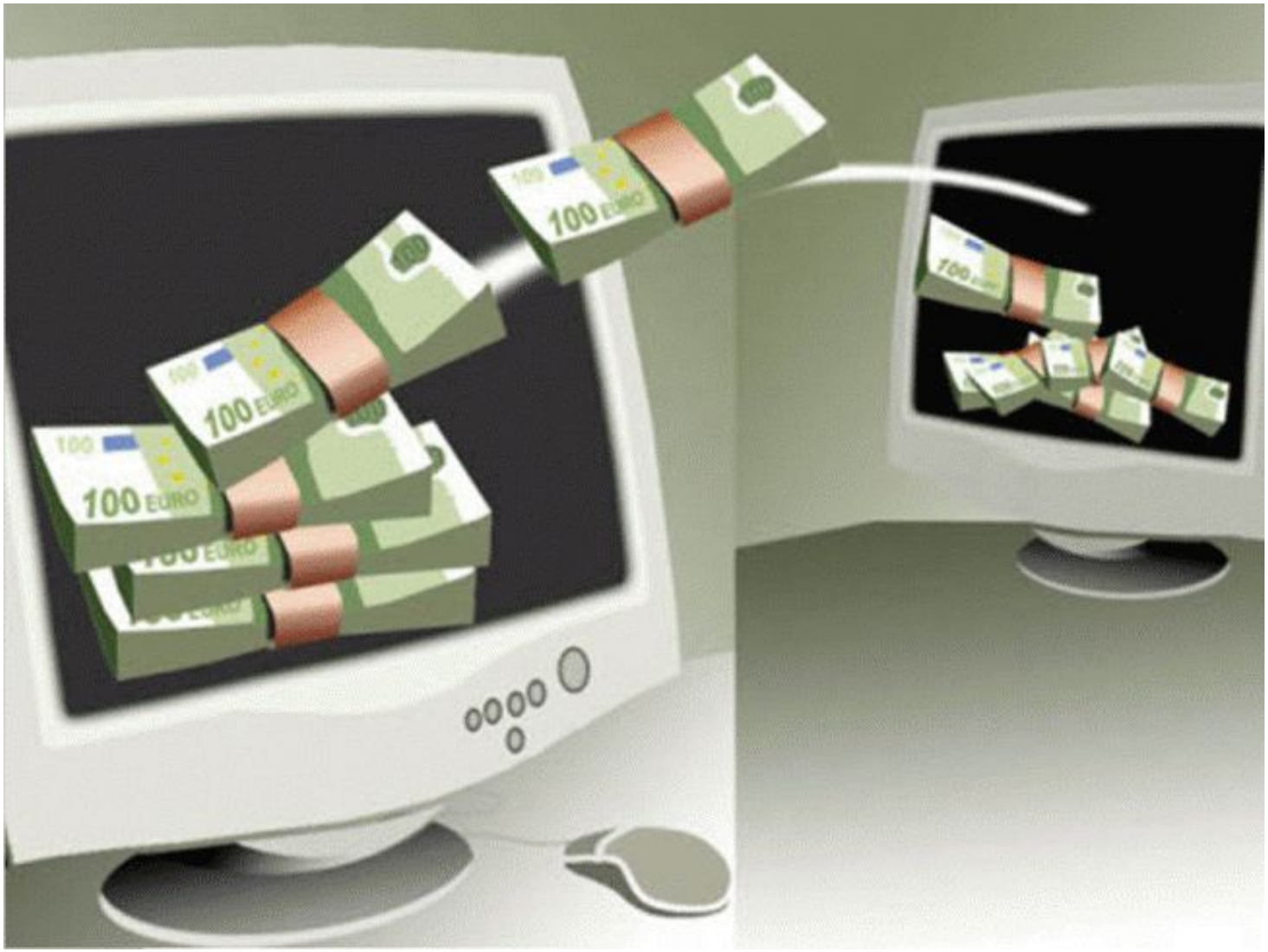
- позвонить в банк-эмитент карты, сообщить о случившемся, и узнать, как можно получить свою карту обратно (застрявшая карта — не всегда признак мошенничества, сбои в банкоматах тоже бывают).

# Банкомат-фантом

# Скотч-метод

# СМС – сообщение

# Удар по кошельку



# Золото Лимпопо

**Madioc Abrams** <madiocbramschamber@gmail.com> 2 июл. в 12:04

Перевести Создать правило Свойства письма кратко

Уважаемый [redacted]

Я послал тебе это письмо месяц назад, но я не уверен, если вы получили его, как я не слышал от вас, и это является причиной, я повторной его. Я Ларри Екрома личный адвокат, чтобы покойный г-н Дема[redacted], бизнес и поставщик химических веществ / масло консультант, который умер вместе с его непосредственным семьи в страшной ДТП 26-го апреля 2007 года. Хранение количество долларов США 13,580.000. 00 млн. был обязан быть процесс передачи на ваше имя, следовательно, я связался с вами. Есть просьба связаться со мной через моего частного адрес электронной почты: madiocbramsat.law@gmail.com как можно скорее представить дополнительные разъяснения по этому вопросу.

с искренним уважением
Madioc Абрамс,

# Общие признаки, по которым можно понять, что вашими данными пытаются завладеть

- только мошенники могут запрашивать номер мобильного телефона и другую дополнительную информацию, помимо идентификатора, постоянного и одноразового паролей;
- только мошенники могут запрашивать пароли для отмены операций или шаблонов. Если вам предлагается ввести пароль для отмены или подтверждения операций, которые вы НЕ совершали, то прекратите сеанс использования услуги и срочно обратитесь в Банк;
- только при мошеннических операциях реквизиты вашей операции не совпадают с реквизитами в полученном SMS-сообщении;
- только на мошеннических сайтах контактный телефон не соответствует официальным;
- на мошеннических сайтах в адресной строке браузера отображаются цифры ip-адреса или любые домены, кроме зарегистрированных доменных имен систем онлайн-банкинга

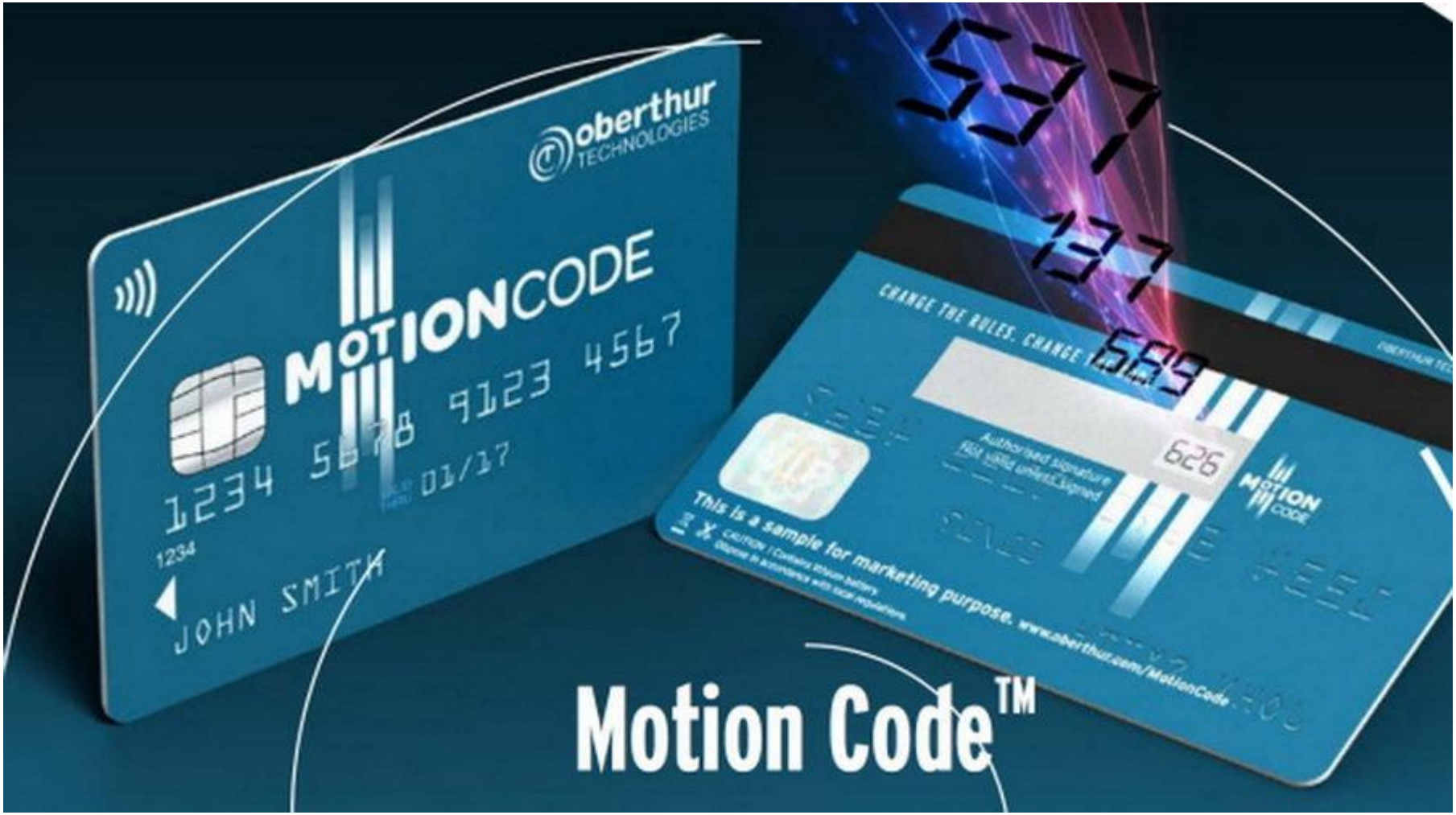
# Карта с биометрической защитой

# Карта с датчиком сердцебиения

# Карта с дисплеем

# Карта «по требованию»

# Карты с меняющимся кодом безопасности



# Финансовые пирамиды

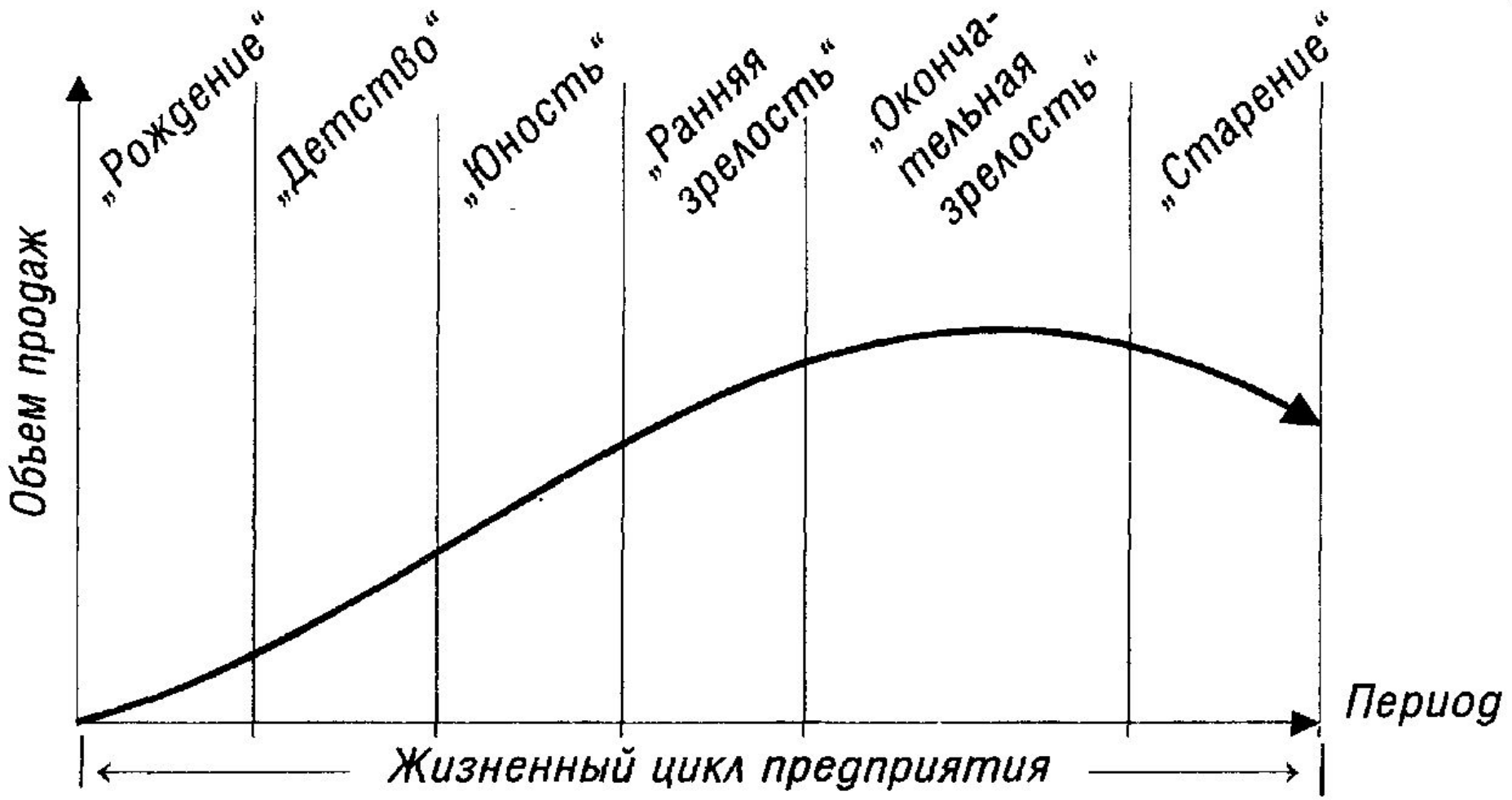
# Общие для всех «финансовых пирамид» признаки

1. отсутствие лицензии ЦБ России или на осуществление деятельности по привлечению денежных средств;
2. обещание высокой доходности, в несколько раз превышающей рыночный уровень;
3. гарантирование доходности (что запрещено на рынке ценных бумаг);
4. массированная реклама в средствах массовой информации, сети Интернет с обещанием высокой доходности;
5. отсутствие какой - либо информации о финансовом положении организации;
6. выплата денежных средств новым участникам из денежных средств, внесенных другими вкладчиками ранее;
7. отсутствие собственных основных средств, других дорогостоящих активов;
8. нет точного определения деятельности организации.

# Виды финансовых пирамид:

- Многоуровневые пирамиды
- Схема Понци в финансовых пирамидах
- Маскирующаяся пирамида
- Матричная пирамида

# Жизненный цикл



# Ответственность за создание финансовых пирамид в РФ

30 марта 2016 года Президент РФ В. Путин подписал Федеральный закон № 78-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации», устанавливающий уголовную ответственность за организацию финансовых пирамид.

Штраф: 1,5 млн. руб.

Срок: 6 лет