# Финансовое мошенничество и риски

Петросян Л. Г., Патраков А. В., Звонилин К. А., Рахмонов У. А., Радонежская Н. В., Ребров И. В.,Литвинова Н.М.,Подпорина С.В.. Масленникова О.М.

# ФИНАНСОВАЯ ГРАМОТНОСТЬ -

это умение рационально распоряжаться финансами.

Большая часть населения имеет недостаточный уровень знаний для понимания основных финансовых продуктов и планирования своего бюджета, недооценивает свои риски и часто принимает неэффективные решения по управлению своими финансами

# ФИНАНСОВОЕ МОШЕННИЧЕСТВО

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

В связи с усложнением механизмов функционирования хозяйственного комплекса мошенничество стало более изощренным и приобрело ярко выраженный интеллектуальный характер

# Основные общие признаки указывающие на риски финансового мошенничества

- ✓ вознаграждение существенно превышает деловую практику по данному типу сделок;
- ✓ использование технологий «социальной инженерии» и манипулирование такими интересами как жадность, желание быстро разбогатеть, зависть;
- ✓ предложение решить все финансовые проблемы в короткий срок;
- ✓ необходимость первоначальных выплат;
- ✓ анонимность контрагента;
- ✓ необходимость мгновенного принятия сложного финансового решения;
- ✓ несоответствие складывающейся ситуации стандартной схеме;
- ✓ наличие указания на эксклюзивный, кастомизированный характер предложения.

# ПРИЧИНЫ РОСТА ФИНАНСОВОГО МОШЕННИЧЕСТВА

## объективные

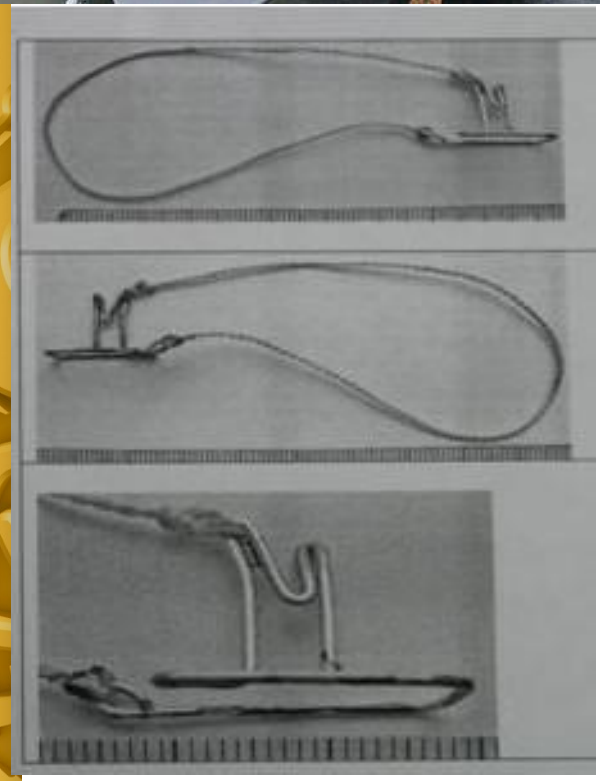
- Финансовый рынок как институт
- Развитие информационных технологий

## Российская специфика

- Идеализация рыночных институтов в 90-е годы (утрата доверия к гос. банкам), отсутствие опыта финансового поведения
- Чрезмерная доверчивость населения и высокая склонность к риску

# Виды финансового мошенничества

Скиммеры

«Ливанская петля»

«Нигерийские письма счастья»

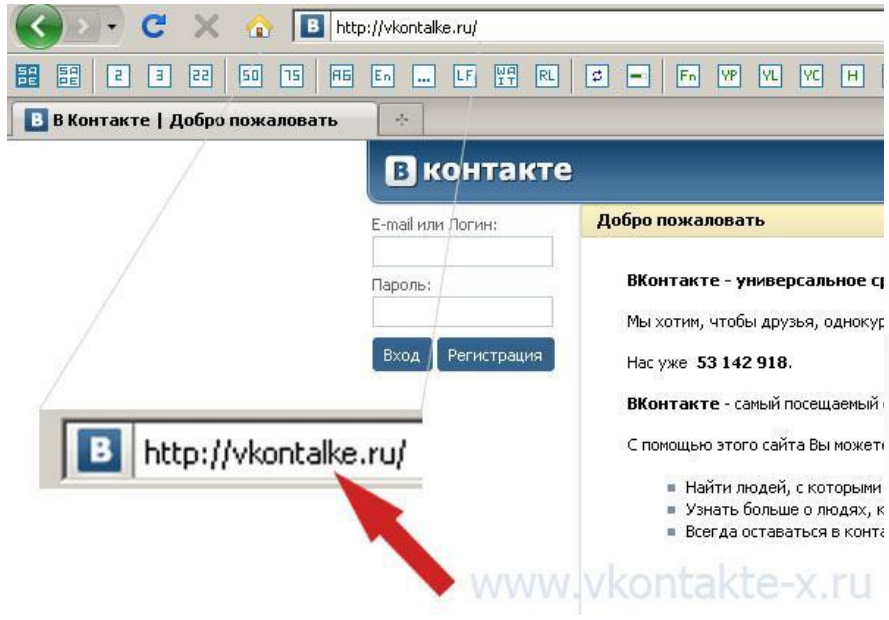

Мошенничество с использованием электронных платежных систем

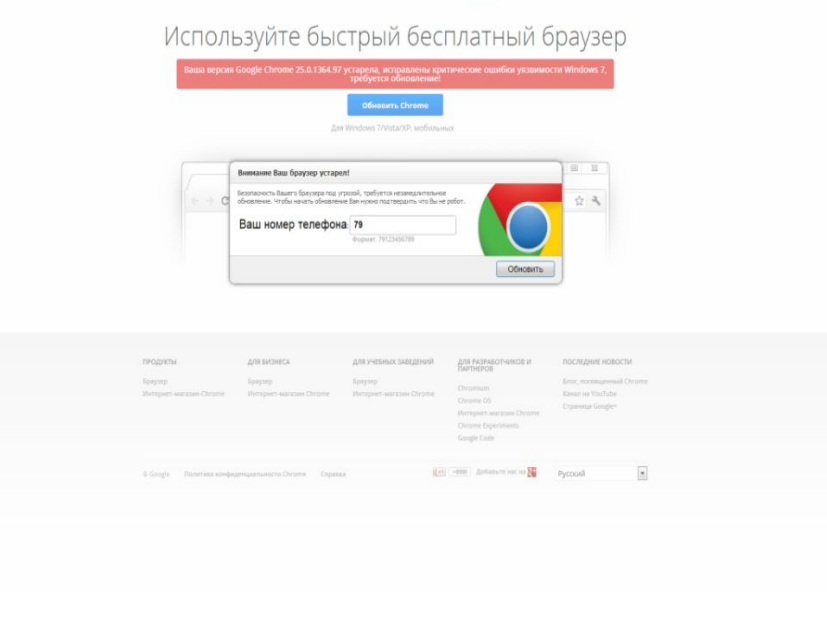
# Виды финансового мошенничества


Мошенничество через взлом аккаунтов в соц. сетях.

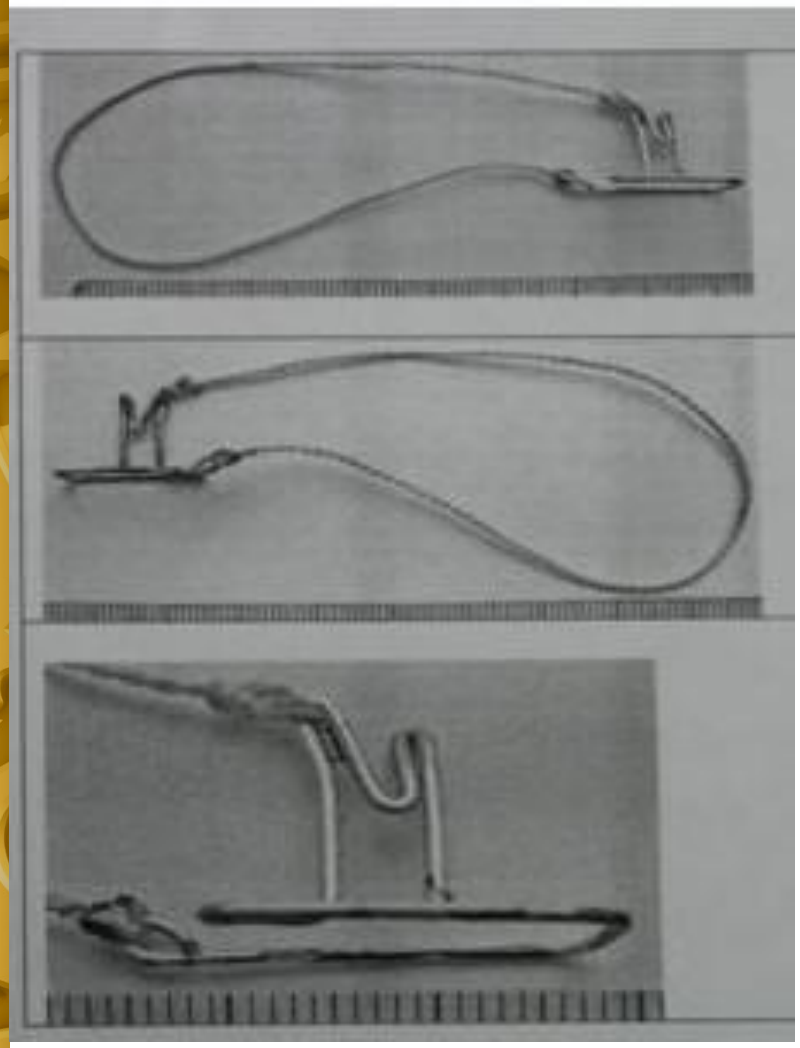
Звонки из «службы безопасности банка».


Фишинговые сайты.



# Скиммеры.



## Ливанская петля

используется для захвата пластиковый карты в банкомате. Сама петля помещается внутрь карта-приёмника, Карта проскакивает внутрь зажима на петле, где и застревает, человек, предполагает, что карта застряла в банкомате от звонившись в службу поддержки уходит. Злодеи Извлекают петлю вместе с картой, после чего соверашют с её помощью покупки.

# Способы противодействия, данным способам, скримминг и ливанская петля мошенничества.

1. Совершать снятие наличных только в отделениях банков, если нет такой возможности, то в торговых центрах, где большой поток людей и шансы успешно установить скриммер низкие.
2. Обращать внимание на сам банкомат, не неоднородности или излишне выступающие части такие как: карта-приёмник, облицовка в районе экрана, панель клавиатуры.
3. При малейшем подозрении извлечь карту, не совершая никакие операции по ней.
4. От звониться в банк и сообщить о предполагаемом нарушении.
5. Если карта была захвачена, немедленно заблокировать счёт и оставить заявление на пере выпуск карты.

# Нигерийские письма счастья, взлом вк, мошенничество с использованием платёжных систем.

Всё вышеперечисленное объединяет, то, что осуществляется через сеть интернет.

**Письма**, нацелены на желающих обогатится быстро и без лишних трудозатрат, в письме упоминается что у жертвы есть, богатый родственник, который умер и завещал огромную сумму денег, однако, что бы переслать завещание и/или перевести деньги на счёт жертве, жертве нужно сначала перевести сумму необходимую за таможенный сбор, зачастую незначительную.

**Взлом вк**, характеризует сообщение от кого-то из списка друзей, с просьбой занять денег под предлогам смертельной опасности близких людей, лица, через аккаунт которого злодей пытается произвести отъём денежных средств.

**Использование платёжных систем,** отличает, что жертве предлагается либо стать частью финансовой пирамиды, либо приобрести товар по сильно заниженной цене, но обязательно по 100% предоплате.

**Фишенговые сайты,** создаются для сбора личной информации, с целью её перепродажи или отъёма денежных средств, через втирания в доверие, так же могут быть попытки шантажа. В строке браузера отсутствует http: соединения или значок: замочка в хроме, щита в фаер фокс. Или сама социальная сеть внезапно выкидывает на экран логина, с просьбой авторизоваться заново.

Общая черта у 1,2 и 3 пункта: после перевода денежных средств, мошенники исчезают, оперативно выводя деньги за рубеж где не представляется возможности их изъять.

# Способ противодействия. Вышеописанным схемам.

1. Вырабатывать критическое мышление. Если у вас внезапно просят денег в долг, спросить, что-то о чём знаете только вы и лицо просящее денег, у мошенников нет времени читать всю переписку.
2. Сомнительно, что уведомление о наследстве придёт на электронную почту, обуздать свою жадность и не открывать письма, с непонятными заголовками. Если в заголовке стоит префикс re: а заголовок письма непонятен не открывать письмо и не скачивать подозрительные файлы, прикреплённые к письму.
3. Цена сильно ниже рыночной, является приманкой, а участие в финансовых пирамидах, в первую очередь должно вызвать вопрос, что гарантии полностью отсутствуют.
4. Обратить внимание на строку браузера, насколько отличается привычный адрес, нет ли лишних букв, не сменился ли домен с .ru на .org .ua .net использовать только защищённое соединение, обязательно иметь антивирус на компьютере.

# Звонки из «службы безопасности банка»

Поступает звонок или с неизвестного номера или с номера идентичного номеру банка. Звонящей представляется: «Сотрудник службы безопасности банка» и спрашивает, совершала ли жертва операцию по списании денежных средств, после того, как жертва сообщает, что такую операцию не проводила, злодей предлагает немедленно сменить протокол защиты карты или карта будет заблокирована, а в отношении жертвы начнётся уголовное расследование. для чего требуется, возможны варианты:

1. Сообщить данные с самой пластиковой карты, **все** цифры и надписи с карты.
2. Продиктовать цифры из пришедшего смс на телефон, которые позволять авторизовать Жертву.
3. Дойти до ближайшего банкомата банка эмитента карты, и совершить ряд операций, которые позволят избежать блокировки карты.

# Способ противодействия. «Звонкам».

1. Не поддаваться панике и не реагировать на давление, злодей может знать многое.
2. Попросить представится, если «сотрудник» не ответил или не назвал из какого банка он звонит, то вешать трубку.
3. Никогда не сообщаться цифры из смс оповещений или с обратной стороны карты.
4. Банку проще заблокировать карту, а вам выдать новую, чем названивать.
5. Банк пришлёт официальное уведомление в виде письма или смс о блокировке карты, без просьбы перезвонить.

# Способы минимизации рисков, общие положения.

## Способы минимизации рисков

- внимательно изучить правила безопасного использования банковской карты
- не сообщать никому, в том числе сотруднику банка, ваши персональные данные и данные банковской карты;
- при возникновении факта мошенничества обратиться в ваше отделение банка
- в случае необходимости заблокировать карту
- не звонить по предложенному в смс номеру телефона по вопросам безопасности вашей карты
- не совершать операции по 100% предоплате с непроверенными контрагентами.
- если вы стали жертвой мошенничества, сразу обращаться в полицию.

# Благодарим Вас за внимание!