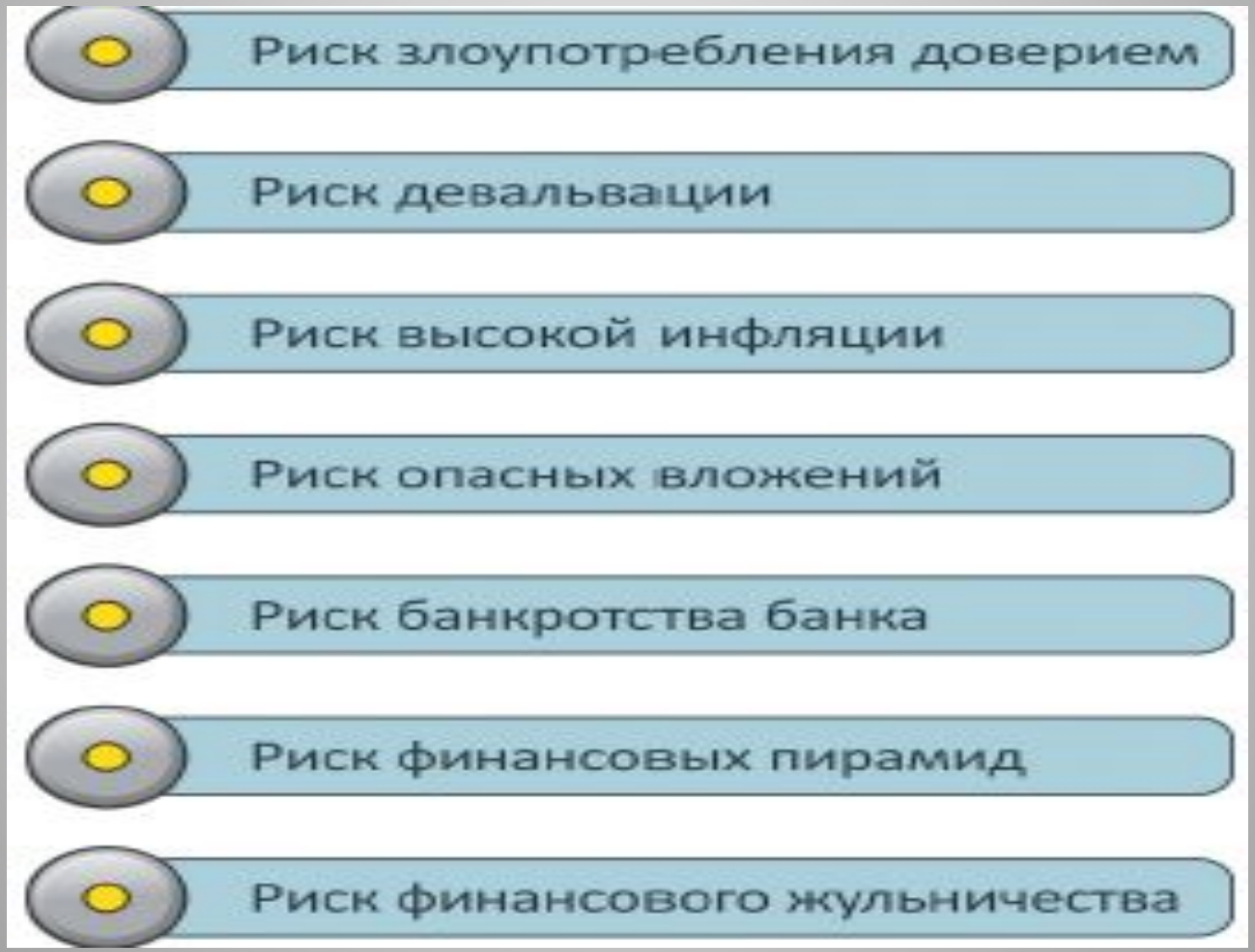
Финансовые риски

это возможность потерять деньги в связи с наступлением каких-либо предвиденных или непредвиденных обстоятельств.

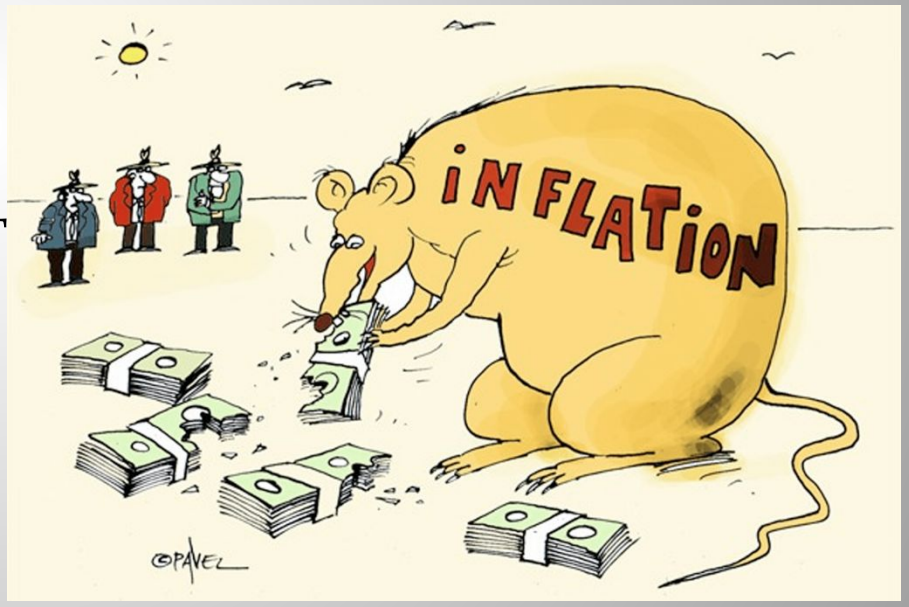
Виды финансовых рисков



РИСК ИНФЛЯЦИИ

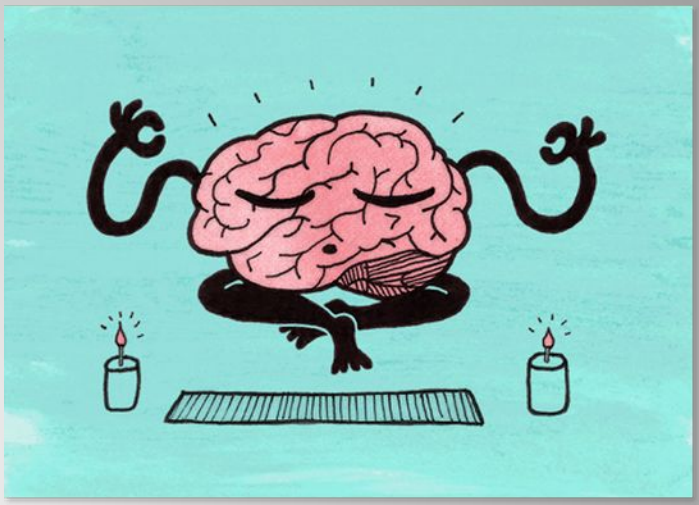
Инфляция — это долговременное устойчивое повышение общего уровня цен на товары и услуги внутреннего рынка.

Риск заключается в том, что сбережения могут обесцениться. Поэтому следует искать способы сохранения накоплений в реальных величинах, например делать вклад в банк с процентной ставкой выше уровня инфляции.



ПОРЕШАЕМ

1. Матвей Николаевич получил в наследство 100 тыс. р. и хранил их дома. Через год он купил на эти деньги мотоцикл. За год инфляция составила 10%. На какую сумму обесценились сбережения Матвея Николаевича за год?



100 000 / 100% * 10% = 10 000 рублей

Ответ: сбережения Матвея Николаевича обесценились за год на 10 000 рублей.

РИСК ДЕВАЛЬВАЦИИ

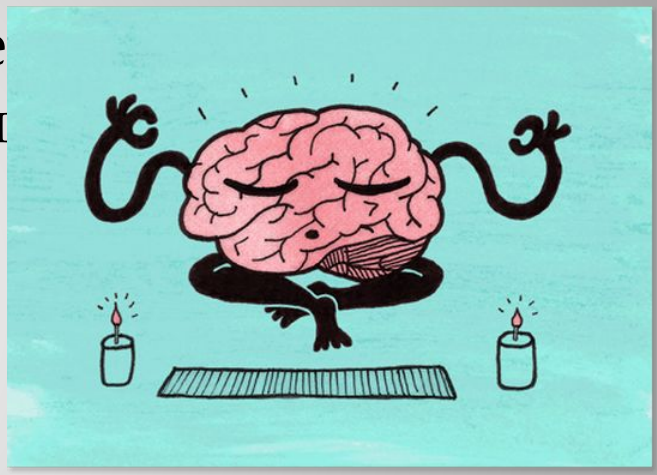
Девальвация представляет собой падение стоимости валюты относительно стоимости золота или других валют.

Актуальна она для тех, кто много путешествует или делает покупки в иностранной валюте.

Если такая ситуация присутствует, можно делать мультивалютные вклады.

ПОРЕШАЕМ

Степанов Илья решил в июне отправиться в путешествие по Австрии. Когда он рассчитывал стоимость своего путешествия, курс составлял 65,50 руб. за евро. В этом случае поездка обошлась бы в 65 500 руб. Но когда он через некоторое время стал покупать билеты на самолёт и заказывать отель, то сумма увеличилась на 4650 руб. Оказалось, что, пока Илья раздумывал о покупке валюты, произошла девальвация рубля.



На сколько рублей увеличился курс евро для россиян за это время?

Посчитаем цену поездки в евро: 65500 / 65,5 = 1000 €
Разница 4650 / 1000 = 4,65 руб.
Ответ: курс евро для россиян увеличился на 4,65 руб.

РИСК БАНКРОТСТВА ФИНАНСОВОЙ ОРГАНИЗАЦИИ

Причины:

1. Внутренние (связаны с деятельностью самой организации: она может быть неэффективной, не отвечать требованиям контролирующей организации, плохо управлять деньгами вкладчиков, использовать мошеннические схемы и пр.)

2. Внешние (обусловлены процессами, протекающими в мировой и национальной экономике. На них мы повлиять не можем)

Следует обратить внимание на рейтинг надёжности, который, например, составляет РА «Эксперт», насколько отличаются условия вклада от средних по стране, есть ли лицензия на осуществление финансовых операций (информацию можно узнать на сайте ЦБ РФ http://www.cbr.ru) и учесть прочие сведения, которые помогут сделать

Страхование вкладов

Создание системы обязательного страхования банковских вкладов физических лиц является специальной гос. программой, которая реализуется в соответствии с ФЗ «О страховании вкладов физических лиц в банках РФ» № 177-ФЗ от 23 декабря 2003 года.

Государством создано Агентство по страхованию вкладов (АСВ), которое возвращает вкладчику сумму его накоплений вместо банка.

Система страхования вкладов работает следующим образом. Банки делают взносы в «общий котел». Если в отношении банка наступает страховой случай (у него отзывается лицензия), то вкладчикам – физическим лицам, в том числе ИП, из этого «котла» АСВ выплачивает денежную компенсацию: возмещение по вкладам определенной суммы.

Согласно закону, возмещение по вкладам в банке, в отношении которого наступил страховой случай, выплачивается клиенту в размере 100% суммы вкладов, но не более 1 400 000 рублей.

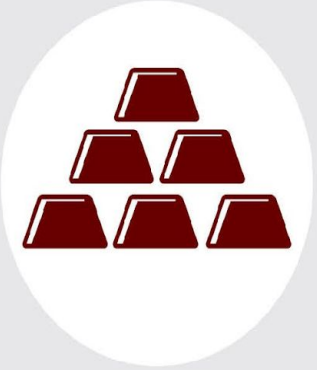
ВКЛАДЫ, КОТОРЫЕ НЕ ПОДПАДАЮТ ПОД СТРАХОВАНИЕ

На предъявителя (в том числе удостоверенные сберегательным сертификатом или сберегательной книжкой на предъявителя)

На счетах адвокатов и нотариусов, если счета открыты для профессиональной деятельности

В филиалах российских банков, находящихся за границей

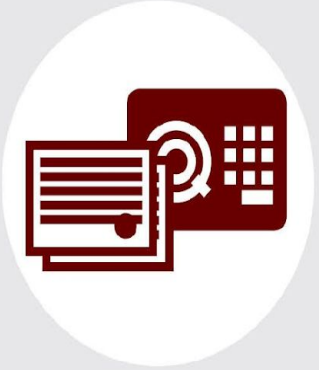
Переданные банкам в доверительное управление



Размещенные на обезличенных металлических счетах

Переведенные в «электронные кошельки»

Размещенные индивидуальными предпринимателями в субординированные депозиты



Размещенные физическими лицами в ценные бумаги банка

РИСК ФИНАНСОВОГО МОШЕННИЧЕСТВА

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

Основными жертвами подобного рода кредитов становятся, как правило, представители социально незащищённых слоёв населения — старики, инвалиды, пьяницы и наркоманы, которым по вполне понятным причинам требуются деньги часто и срочно. При этом они зачастую просто не в состоянии здраво оценить последствия.

ПОСЧИТАЕМ

3. Варвара Леонидовна оказалась в сложной ситуации: её сын попал в аварию и срочно понадобились деньги на операцию. Поскольку она была художником и зарабатывала только продажей своих картин, не имея постоянной работы, все банки в кредите ей отказали. Она обратилась в Кредитный союз «Выручаю», где ей предложили 120 тыс. р. под 1,5% в день. Сколько придётся переплатить Варваре Леонидовне за кредит в этой компании?

Стоимость кредита в день составит 120 000 / 100% * 1,5% = 1800 руб.

Ответ: Варваре Леонидовне придется платить за кредит ежедневно 1800 рублей, общая переплата составит 1880 х дни,

Личная финансовая безопасность. Защита от финансового мошенничества

Финансовая безопасность как залог финансового здоровья

Наша финансовая безопасность напрямую зависит от принимаемых нами ежедневно решений. Непродуманный выбор поставщика финансовых услуг, невнимательное чтение условия договоров, отсутствие финансовой дисциплины и - как следствие - неприятная финансовая ситуация.

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

- **Финансовые пирамиды**
- **Телефонные мошенничества**
- **Интернет- мошенничества**
- **Мошенничества с использованием банковских карт**

Финансовые мошенники переключились на детей и молодежь

Банк России, Директор департамента противодействия недобросовестным практикам Валерий Лях:

«Сегодняшние мошенники в финансовой сфере с пенсионеров переключились на детей и молодежь . Изменили они и способы завлечения в свою сеть. В интернете появились целые схемы, рассчитанные именно на них. Например, в мобильных играх и приложениях.»

По оценкам Банка России за прошлый год заблокировали более 800 страниц в интернете, чья деятельность попадала под определение **"мошенничество"**,в том числе **160** лжебанков**, 62 -** лже-МФО, **111 -** лже-страховщиков **и**
45 финансовых пирамид.

Формы мошенничества и способы минимизации рисков

I. Финансовые пирамиды

Финансовые пирамиды : бесконечная история

-Одна из первых финансовых пирамид появилась еще в 1720 году. Джон Ло своей «Миссисипской компанией» разорил всю Францию.

- Россия и страны СНГ познакомились с такими финансовыми структурами лишь в начале 90-х.

Финансовая пирамида - это такая структура, в которой доход извлекается путем формирования денежных поступлений от привлечения все большего количества инвесторов.

Доход распределяется в первую очередь между участниками финансовой пирамиды, которые вступили в нее самыми первыми. Основной чертой финансовой пирамиды является то, что вкладчикам обещается высокая доходность по их вкладам. Выплаты процентов осуществляются не за счет полученной от инвестиций прибыли, а за счет вкладов следующих участников. Деньги, вращающиеся в пирамиде, на самом деле ничем не подкреплены, а потому рано или поздно, такая структура не сможет обеспечить выплаты всем участникам, причем не только процентов, но даже непосредственно вкладов.

Финансовая пирамида

Постоянное привлечение денежных средств

- Финансовая пирамида – это социально-экономическая система, основывающаяся на постоянном привлечении денежных средств участников под обещания нерыночно высокой доходности, без реальной деловой цели инвестирования

Доход есть пока существует приток денег

- Доход организаторов пирамиды и выплаты инвестиционного дохода участникам формируется до тех пор пока существует приток от новых участников

Стимулирование притока денег из взносов новых участников

- В многоуровневых пирамидах привлечение участников стимулируется денежными выплатами из взносов новых участников

От ее деятельности в 1994 г. пострадало больше 15 млн человек. Успех «МММ» вызвал появление около 1700 других финансовых пирамид, таких как «Русский дом Селенга», «Хопёр-Инвест» и другие.

В 2011 году Мавроди создал интернет-пирамиду международного масштаба под старым названием МММ. Более 300 тыс. человек из США, Латинской Америки, России, Европы оказались обманутыми.

Финансовые пирамиды в России: учимся ли мы на своих ошибках ?

«Это одна из самых масштабных финансовых пирамид, которую мы выявили за последние годы, она развернула свою деятельность во многих регионах, практически по всей стране. Причём, в последнее время рекламирует себя все более активно, стараясь вовлечь как можно больше граждан», — говорит директор департамента противодействия недобросовестным практикам ЦБ Валерий Лях.

По мнению регулятора, деньги привлекаются и в рублях, и в криптовалюте, но при этом признаки реальной экономической деятельности отсутствуют. ЦБ сообщил, что компании группы «Кэшбери» строят свою деятельность на принципах сетевого маркетинга, обещают завышенную доходность, ведут агрессивную рекламу в СМИ и социальных сетях. Лицензий Банка России у компаний, которые предлагают финансовые услуги, нет.

Финансовые пирамиды: основные признаки

http://www.kp.ru/daily/26272.3/3148966

Волны финансовых пирамид в Российской Федерации

Период	Примеры
Первая волна 1993 – 1998 гг.	«МММ», «Хопер-Инвест», «Властилина», Банк «Чара», «Русский дом Селенга», ГКО
Вторая волна 2008 – 2011 гг.	ООО «Золотая лига», «Глобал», «РуБин», «Бинар», МММ-2011, КПК РОСТ, Российская социальная программа.
Третья волна 2013 – н.в.	MBM.Partners, Impetra Plus, Академия Победителей, Сберкарта, Give1 Get4, SETinBOX , Руссинвест, РСП

Причины, заставляющие людей участвовать в финансовых пирамидах

> 50%

людей сознательно участвуют в финансовых пирамидах с целью заработка

< 50%

людей характеризуются низкой финансовой грамотностью.

Телефонные мошенничества

Звонок или СМС с незнакомого номера

СМС с информацией о выигрыше и предложением направить ответное СМС, позвонить, отписаться от рассылки	Вам звонят не друзья, а мошенники. Их цель - ваши деньги
СМС от якобы друга/родственника с просьбой срочно перевести деньги	Ответное СМС, звонок оказываются платными и очень дорогими
СМС со ссылкой, по которой нужно обязательно перейти	Вы попадаете на «фишинговый» сайт, он скачивает вашу личную информацию
СМС с информацией, что у вас задолженность по кредиту и просьбой перезвонить по указанному номеру	Мошенники выспрашивают у вас конфиденциальную информацию

Ваши действия:

Удалять СМС подобного содержания с незнакомых номеро

- Перезванивать на реальные телефоны друзей и родственн
- Отказываться от затяжных разговоров по странным темам

Интернет-мошенничества

По электронной почте с незнакомого адреса

О получении вами очень хорошей работы за рубежом, только надо оплатить визу, страховку, стажировку и т.п.

О получении вами приза, выигрыша, только сначала надо заплатить налоги, комиссионные и т. п.

Вам пишут не друзья, а мошенники. Их цель - ваши деньги.

О необходимости перехода по ссылке, приведенной в письме.

Вы попадаете на «фишинговый» сайт, он скачивает вашу личную информацию.

С просьбой помочь перевести крупную сумму денег из-за рубежа, за что вы получите % от суммы, только надо оплатить какие-то услуги, таможню и т.п.

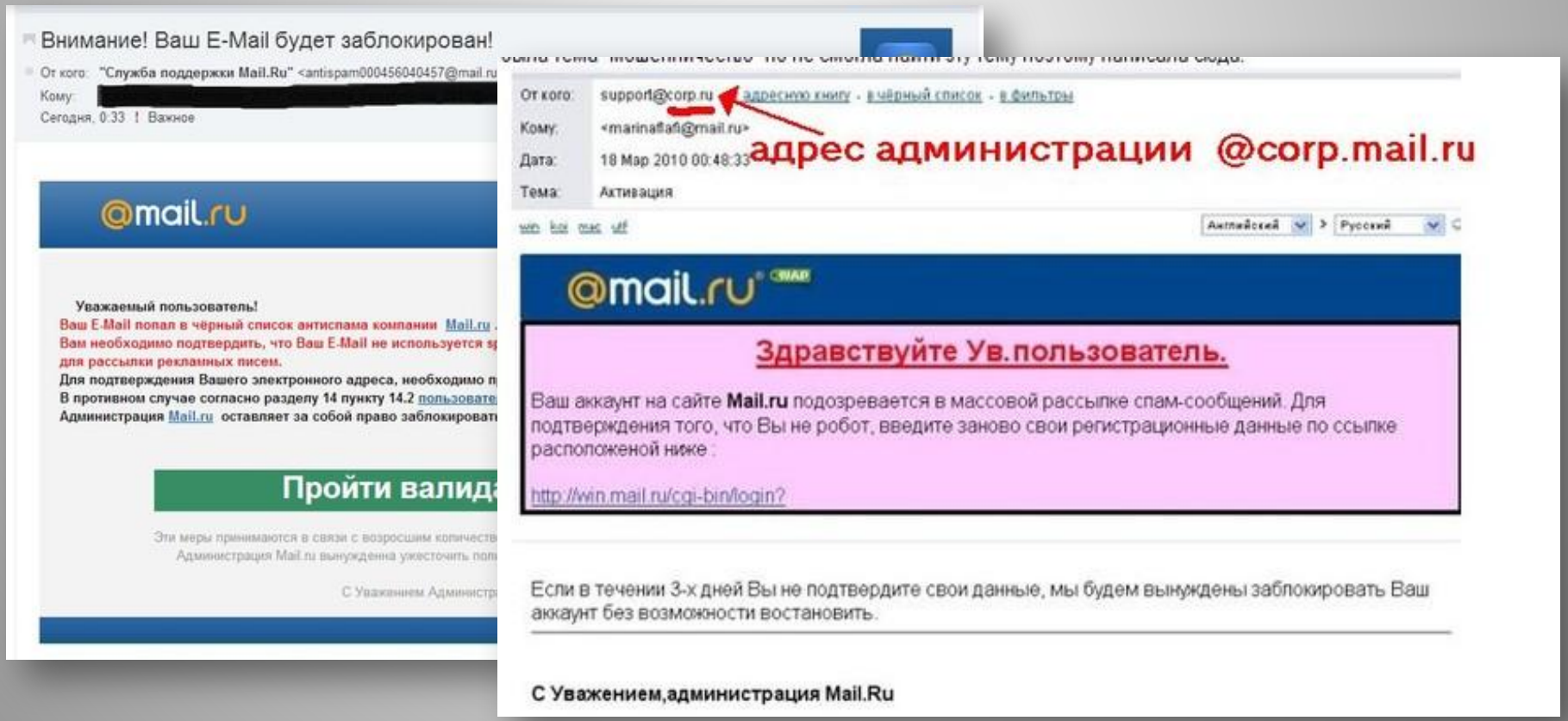
Ваши действия: удалять письма подобного содержания с незнакомых адресов, не читать, не отвечать, не проходить по указанным в них ссылкам.

Формы мошенничества

III. Кибермошенничество

Терминология

Фишинг (англ. phishing) – это технология интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских и идентификационных карт, посредством спамерской рассылки или почтовых червей.



Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

Фишинг:

- а) почтовый
- б) онлайновый
- в) комбинированный

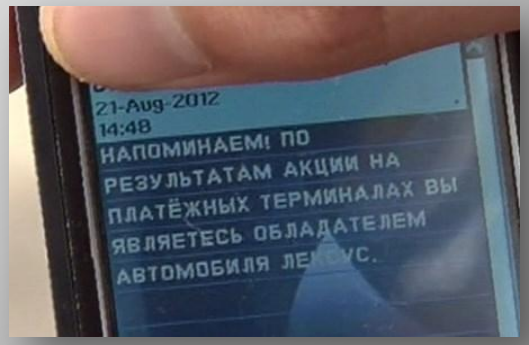
Способы минимизации рисков

- проявлять осторожность
- застраховать карту от риска мошенничества
- использовать разные инструменты для разных видов расчетов
- использовать метод многофакторной аутентификации

Терминология

Вишинг (англ. vishing) – это технология интернет-мошенничества, заключающаяся в использовании автонабирателей и возможностей интернет-телефонии для кражи личных конфиденциальных данных, таких как пароли доступа, номера банковских и идентификационных карт и т.д.

Смишинг – это вид мошенничества, при котором пользователь получает СМС-сообщение, в котором с виду надежный отправитель просит указать какую-либо ценную персональную информацию (например, пароль или данные кредитной карты). Смишинг представляет собой подобие фишинга, при котором мошенниками с той же целью рассылают электронные письма.



Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

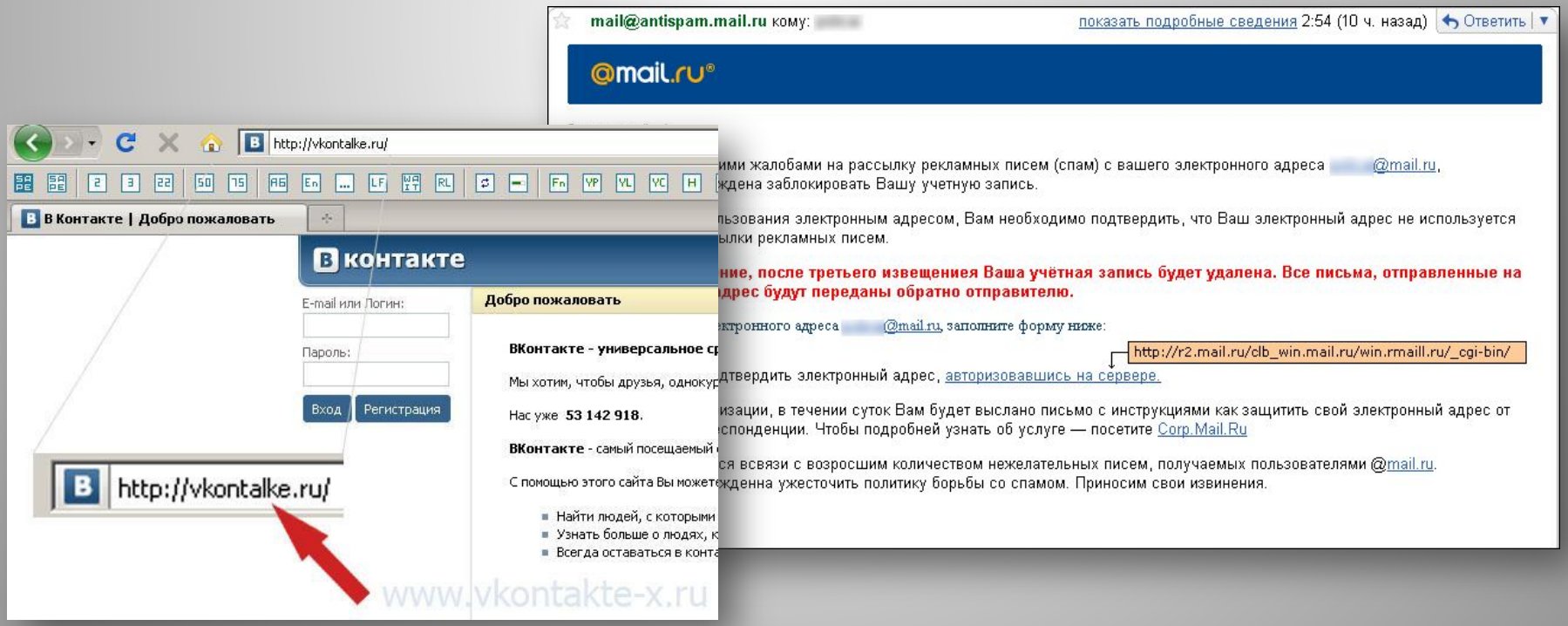
- Вишинг
- Смишинг

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

Терминология

Фарминг (англ. pharming) – более продвинутая версия фишинга, заключающаяся в переводе пользователей на фальшивый веб-сайт и краже конфиденциальной информации.



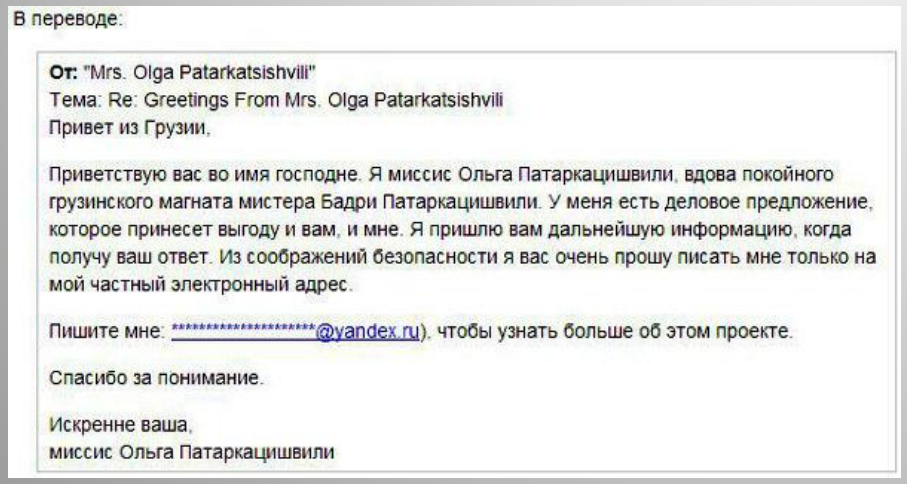
Формы мошенничества и способы минимизации рисков

III. Кибермошенничество	Способы минимизации рисков
Фарминг	• установка антивирусной программы • установка обновлений от производителей ПО и поставщика услуг Интернета. • проверка URL • проверка изменения адреса http на https при переходе на страницу оплаты

Терминология

«Нигерийские письма» (англ. «Nigerianscam») – электронное письмо с просьбой о помощи в переводе крупной денежной суммы, из которой 20-30% должно получить лицо, предоставляющее счет. При этом получателю необходимо срочно 6-10 тысяч долларов США отправить по системе электронных платежей по требованию адвоката.

Как разновидность используется рассылка о выгодном капиталовложении или устройстве на высокооплачиваемую работу, получении наследства или иных способах быстрого обогащения при условии совершения предварительных платежей.



В переводе:

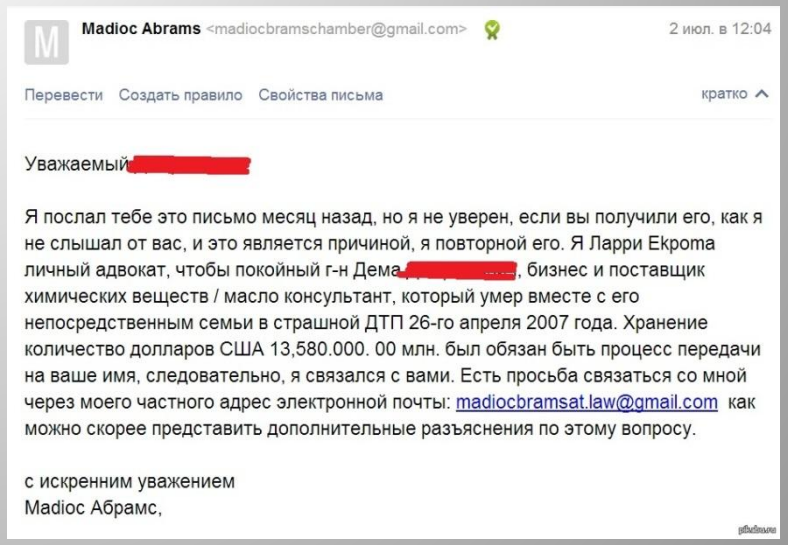
От: "Mrs. Olga Patarkatsishvili"
Тема: Re: Greetings From Mrs. Olga Patarkatsishvili
Привет из Грузии,

Приветствую вас во имя господне. Я миссис Ольга Патаркацишвили, вдова покойного грузинского магната мистера Бадри Патаркацишвили. У меня есть деловое предложение, которое принесет выгоду и вам, и мне. Я пришлю вам дальнейшую информацию, когда получу ваш ответ. Из соображений безопасности я вас очень прошу писать мне только на мой частный электронный адрес.

Пишите мне: **********@yandex.ru), чтобы узнать больше об этом проекте.

Спасибо за понимание.

Искренне ваша,
миссис Ольга Патаркацишвили



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,

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество	Способы минимизации рисков
«Нигерийские письма»	• установить антиспамерские программы • критически относиться к предложениям получения быстрого и необоснованного дохода • получить консультацию экспертов в области финансового мошенничества • проявлять осмотрительность при принятии быстрых финансовых решений

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

- Интернет-аукцион
- Электронная торговля
- Скандинавский аукцион
- Семь кошельков
- С помощью платежной системы

Способы минимизации рисков

- пользуйтесь проверенными мировыми и российскими торговыми площадками
- заключайте сделку только через выбранную площадку
- требуйте максимально полной информации о продавце дешевого товара
- по возможности оплачивайте товар по факту его получения

Мошенничество с PayPal*

1. Вы разместили объявление о продаже
2. Мошенник высылает Вам письмо с предложением купить товар, иногда за большую цену и не для себя
3. Вы просите перевести деньги
4. Мошенник просит вас указать адрес, зарегистрированный в PayPal и говорит что выслал деньги туда, но они появятся на счёте в PayPal, когда вы введете номер почтового отправления
5. К вам приходит письмо, похожее на PayPal
6. Вы отправляете товар и вводите номер отправления в указанную в письме страницу

Товара у вас нет. Претензии выставлять некому

*PayPal - крупнейшая дебетовая электронная платёжная система
Аналоги в РФ: Яндекс.Деньги, WebMoney

Терминология

Кликфрод (от англ. click fraud) — один из видов сетевого мошенничества, представляющий собой обманные клики на рекламную ссылку лицом, не заинтересованным в рекламном объявлении. Может осуществляться с помощью автоматизированных скриптов или программ, имитирующих клик пользователя по рекламным объявлениям Pay per click.

Кликджекинг (от анг. clickjacking) механизм обмана пользователей интернета, при котором злоумышленник может получить доступ к конфиденциальной информации или даже получить доступ к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу.

Виды кликфрода

технические клики

клики рекламодателей

клики конкурентов

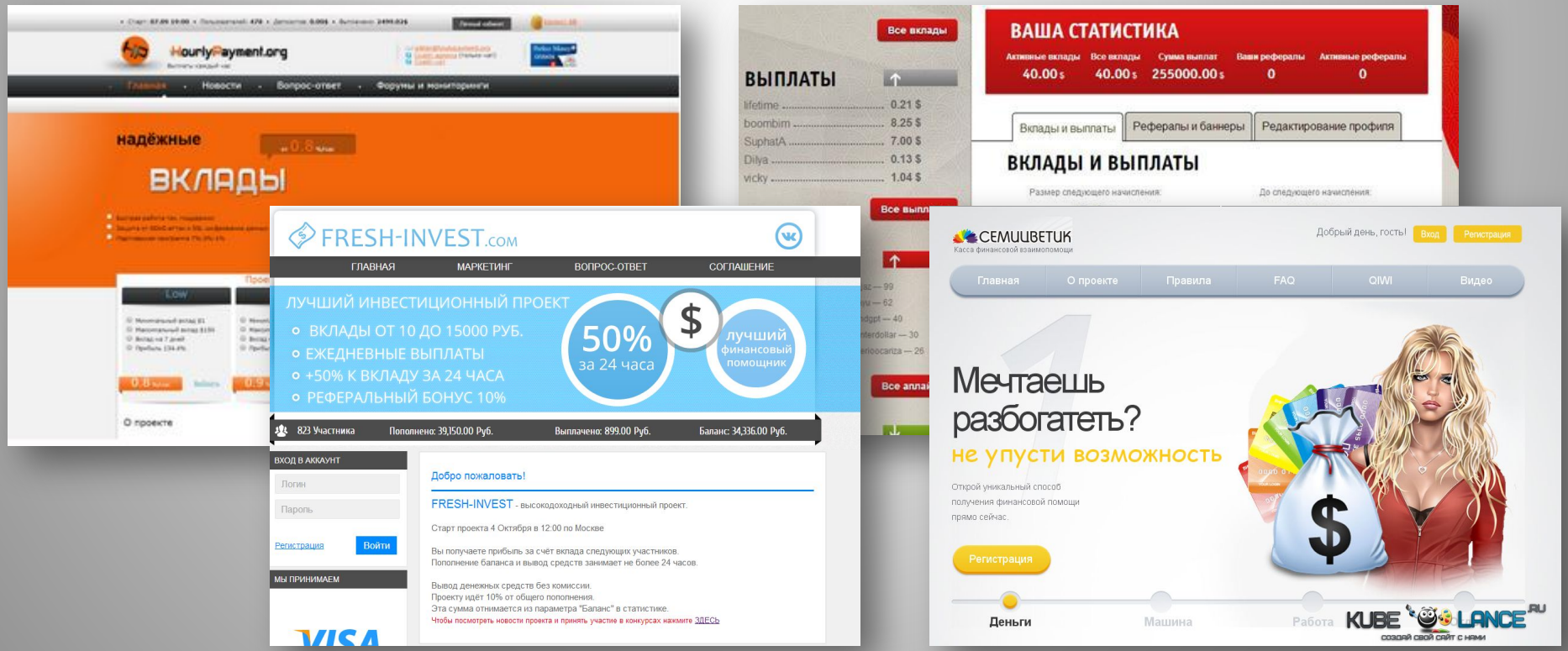
клики со стороны недобросовестных веб-мастеров

Терминология

PAMM-счета (от англ. Percent Allocation Management Module – модуль управления процентным распределением) – специфичный механизм функционирования торгового счёта, технически упрощающий процесс передачи средств на торговом счёте в доверительное управление выбранному доверенному управляющему для проведения операций на финансовых рынках.

Терминология

Хайп (англ. HYIP, High yield investment program) – это высокодоходная инвестиционная программа, капитал которой формируется из взносов пользователей сети Интернет.



Формы мошенничества и способы минимизации рисков

III. Кибермошенничество	Способы минимизации рисков
Хайп	• провести «тестовый режим» участия в хайп-проекте • анализировать информацию сайтов-мониторингов и форумов, освещающих состояние дел по интересующему вас хайп-проекту • распределять денежные средства между несколькими хайп-проектами • не инвестировать заемные средства • не инвестировать «последние деньги»

Формы мошенничества и способы минимизации рисков

IV. Мошенничество в социальных сетях

- Сетевые домушники
- Интернет-угонщики
- Сетевые грабители

Способы минимизации рисков

- проявлять должную осмотрительность при выкладывании в сеть личных данных
- ограничить доступ незнакомых людей к информации, потенциально интересной для мошенников
- не публиковать «горячую» информацию, находясь в отпуске

Формы мошенничества и способы минимизации рисков

II. Мошенничество с использованием банковских карт

а) offline:

- банкоматы и терминалы (в т.ч. скимминг)
- оплата в магазинах или ресторанах

Способы минимизации рисков

- пользоваться только банкоматами, установленными в безопасных местах
- внимательно осматривать банкомат, перед его использованием
- закрывать клавиатуру при вводе пин-кода
- оформить услугу SMS-оповещения о проведенных операциях по карте
- не давать согласие на получение карты по почте и ее активации по телефону
- не хранить пин-код вместе с картой
- не сообщать по мобильным или стационарным телефонам реквизиты карты и ее пин-код
- определить лимит суточного снятия наличных по карте
- блокировать карту немедленно в случае утери/хищения

Мошенничества с банковскими картами

При совершении платежей с использование м банкоматов

Скимминг - кража данных с помощью различных замаскированных устройств, устанавливаемых на банкомат. За банкоматом ведется видеонаблюдение с целью получения PIN-кода.

Траппинг - блокировка карты в банкомате с помощью различных устройств. Карта извлекается мошенником непосредственно после ухода владельца и используется с применением PIN-кода, полученного с видеозаписи.

Скотч-метод - прикрепленный к диспенсеру двухсторонний скотч не дает получить банкноты.

Ваши действия

Проявлять осторожность, обращать внимание на посторонних вокруг, на подозрительные устройства, накладки в местах ввода PIN-кода и

Формы мошенничества и способы минимизации рисков

II. Мошенничество с использованием банковских карт

б) online:

- интернет-мошенничества

Способы минимизации рисков

- установить программы защиты и обеспечения безопасности компьютера в Интернете
- проводить финансовые операции только с защищенных веб-сайтов
- не сообщать пароль доступа к своему счету через интернет
- использовать надежные пароли
- по окончании работы выходить из учетной записи
- не отвечать на электронные сообщения с запросом на изменение параметров защиты
- использовать разные инструменты для разных видов расчетов

Формы мошенничества и способы минимизации рисков

Как заблокировать карту на примере ЦБ РФ

Через сотрудников отделения банка

Через контактный центр или клиентскую службу*

Через сервис Мобильный банк

Через Сбербанк-Онлайн

* Позвонив по номеру 8-800-555-55-50; 8-800-200-37-47 заблокировать карту при ее нахождении может и третье лицо

Правила платежной безопасности

Незамедлительно сообщать в платежную организацию, если «взломан» кошелек

ден ги.

При пользовании банкоматом проявлять осторожность, обращать внимание на

V. Другие виды финансового мошенничества

брачные аферы

нелегальные азартные игры

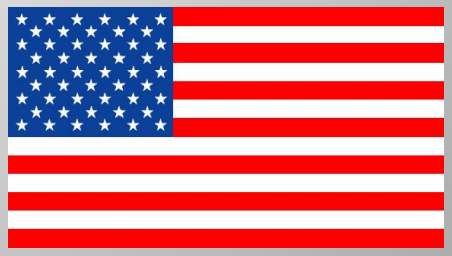
раздолжнители

махинации с арендой/покупкой недвижимости или автомобилей

использование чужих паспортов для сомнительных сделок

Современный опыт законодательной борьбы с финансовым мошенничеством

Уголовное законодательство многих зарубежных стран имеет специальные нормы, посвященные уголовной ответственности за мошенничество.



Современный опыт законодательной борьбы с финансовым мошенничеством

Особенностью российского законодательства является то, что в нем **нет специальных норм по противодействию финансовому мошенничеству.**

Статья 159 УК РФ Мошенничество

Штраф	• исправительные работы • принудительные работами	• ограничение свободы • арест • лишение свободы

один или группой лиц	с использованием служебного положения	мошенничество с недвижимостью и в сфере предпринимательской деятельности

Современный опыт законодательной борьбы с финансовым мошенничеством

- Статья 159.1 УК РФ Мошенничество в сфере кредитования
- Статья 159.2 УК РФ Мошенничество при получении выплат
- Статья 159.3 УК РФ Мошенничество с использованием платежных карт
- Статья 159.5 УК РФ Мошенничество в сфере страхования
- Статья 159.6 УК РФ Мошенничество в сфере компьютерной информации

ВЫВОДЫ

1. Существует большое количество финансовых рисков.
2. При выборе линии своего финансового поведения необходимо учитывать их влияние и стараться свести его к минимуму.
3. Чтобы в каждом конкретном случае минимизировать риски, следует выбирать определённые финансовые инструменты и быть осмотрительными при выборе финансовой организации.
4. При вступлении в отношения с небанковскими кредитными организациями необходимо обязательно просчитывать свои финансовые обязательства.