

Финансовые риски

ЭТО ВОЗМОЖНОСТЬ
потерять деньги
в связи с
наступлением
каких-либо
предвиденных
или
непредвиденных
обстоятельств.



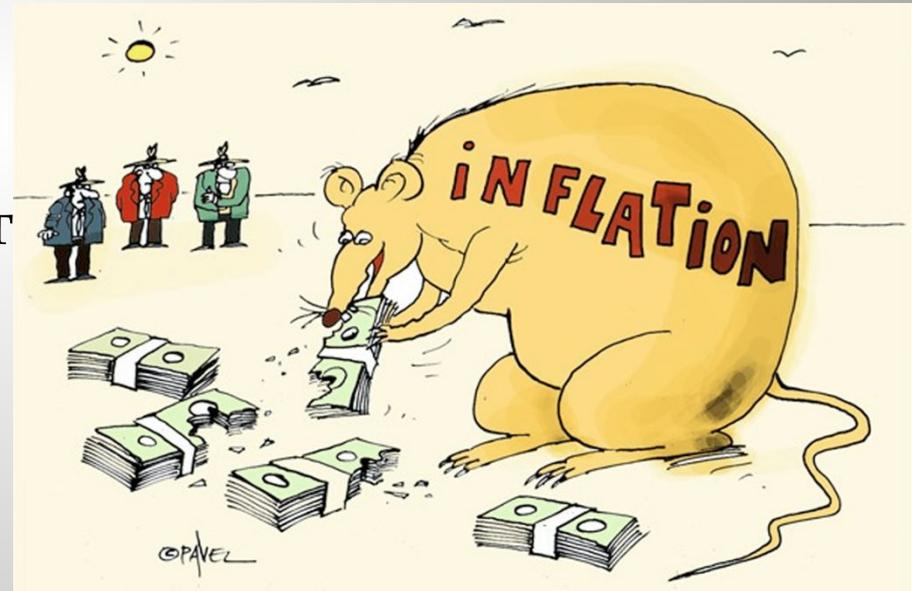
Виды финансовых рисков

- Риск злоупотребления доверием
- Риск девальвации
- Риск высокой инфляции
- Риск опасных вложений
- Риск банкротства банка
- Риск финансовых пирамид
- Риск финансового жульничества

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?



$$100\ 000 / 100\% * 10\% = 10\ 000 \text{ рублей}$$

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.

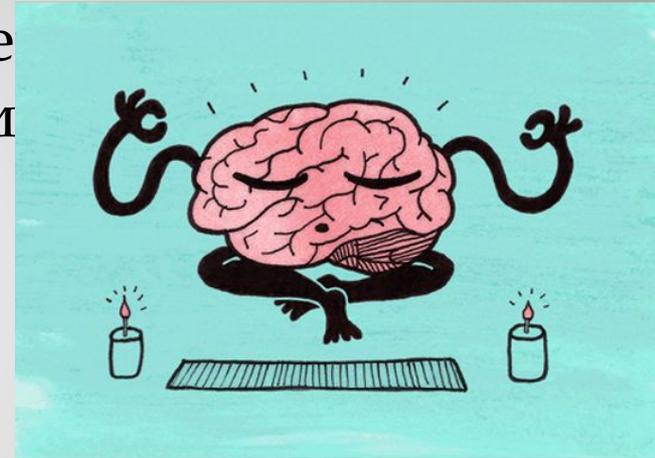
Актуальна она для тех, кто много путешествует или делает покупки в иностранной валюте.

Если такая ситуация присутствует, можно делать мультивалютные вклады.



ПОРЕШАЕМ

Степанов Илья решил в конце
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: $65500 / 65,5 = 1000 \text{ €}$

Разница $4650 / 1000 = 4,65 \text{ руб.}$

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

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

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)



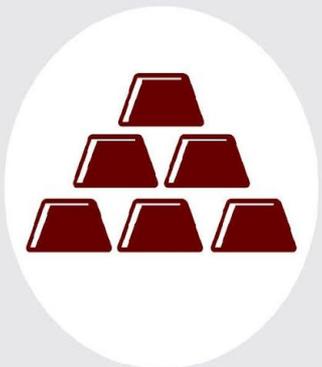
На счетах адвокатов и нотариусов, если счета открыты для профессиональной деятельности



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

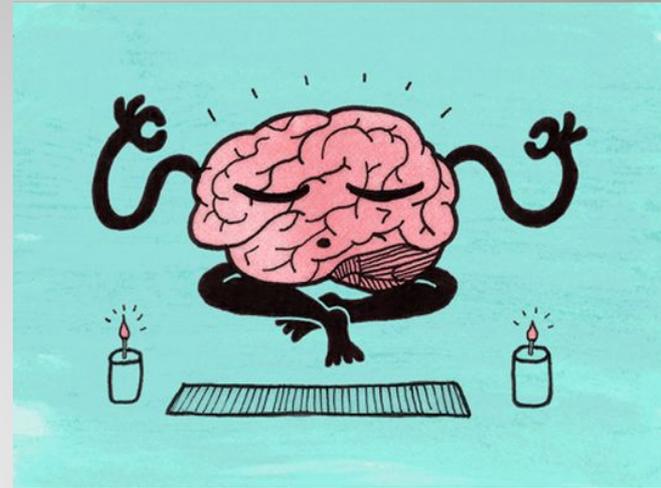
Финансовое мошенничество – совершение противоправных действий в сфере денежного обращения путём обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

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 придётся 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

**Финансовая грамотность -
это уверенность в своём
будущем!**



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

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

ПЯТЬ ОСНОВНЫХ ПРИЗНАКОВ ФИНАНСОВОЙ ПИРАМИДЫ

1 **Сверхвысокий доход.**

Все, что больше 20 - 30% в год, - это заведомо неправда. Гарантировать (именно гарантировать, а не обещать) такую прибыль могут только мошенники.



2

Секретные технологии.

Как правило, строители пирамид очень туманно рассказывают о том, чем они конкретно занимаются. Обычно это подается как некая тайна, о которой знают только избранные. Но вас готовы в нее посвятить... За небольшую плату.



3

Офиса нет либо он явно временный.

Связь с организаторами осуществляется только по телефону и электронной почте. Деньги переводятся электронным платежом. Некоторые принимают средства от населения и наличными. Но это уже прошлый век.



Дмитрий ПОЛУХИН



4

Обещание щедрых комиссионных за привлечение новых клиентов.

Некоторые легальные компании работают по этой же схеме. Но обычно в таком случае есть конкретный продукт, который предлагается продавать.



5

Агрессивная рекламная кампания.

Обычно упор в ней делается на желание большинства людей стать богатыми как можно быстрее и не прикладывая к этому никаких усилий.

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.	МВМ.Partners, Impetra Plus, Академия Победителей, Сберкарта, Give1 Get4, SETinBOX, Руссинвест, РСП



НОВАЯ ПРОГРАММА АЛЬТЕРНАТИВЫ КРЕДИТУ

ПОДДЕРЖИТ РОССИЯН В ПЕРИОД КРИЗИСА!

С целью поддержки населения России в сложной экономической ситуации, компания «РСГ ГРУП» предлагает новую «социальную программу стабильности».

«РСГ ГРУП» не зависит от курса доллара, роста цен и других внешних факторов.

Среди других преимуществ: минимальный пакет документов для рассмотрения заявки (паспорт и ИНН), досрочное погашение без штрафных санкций, выплаты до 30 лет.

Справка о доходах не требуется!

Томск, пр-т Кирова, 51-А, строение 15, офис 206 (б. «Дипломат») Звоните: 8-3822-30-32-46, 90-30-58, 8-913-850-32-46 www.altercredit.ru

Посредничество в торговле авто и недвижимостью. ООО «РСГ ГРУП», ИНН 6001010001 ОГРН 1026000000000 от 18.07.2014. Адрес: 600001 г. Томск. Не является кредитной организацией.



Причины, заставляющие людей участвовать в финансовых пирамидах

> 50%

людей сознательно участвуют в финансовых пирамидах с целью заработка

< 50%

людей характеризуются низкой финансовой грамотностью.

Звонок или СМС с незнакомого номера

Телефонные мошенничества

СМС с информацией о выигрыше и предложением направить ответное СМС, позвонить, отписаться от рассылки

СМС от якобы друга/родственника с просьбой срочно перевести деньги

СМС со ссылкой, по которой нужно обязательно перейти

СМС с информацией, что у вас задолженность по кредиту и просьбой перезвонить по указанному номеру

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

Ответные СМС, звонок оказываются платными и очень дорогими

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

Мошенники выспрашивают у вас конфиденциальную информацию

Ваши действия:

- Удалять СМС подобного содержания с незнакомых номеров
- Перезванивать на реальные телефоны друзей и родственников
- 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.

О необходимости перехода по ссылке, приведенной в письме.

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



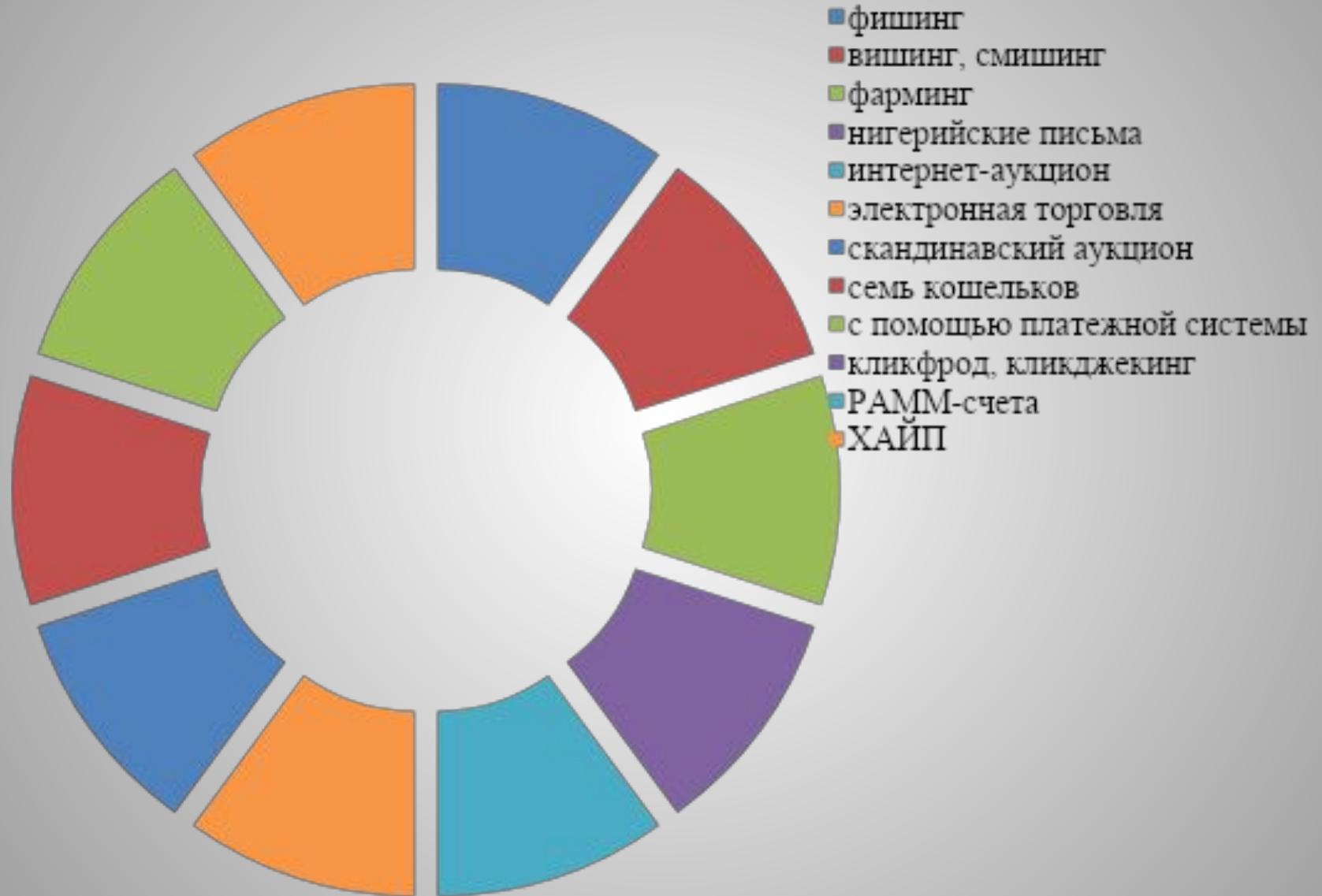
Вам пишут не друзья, а мошенники. Их цель - ваши деньги.

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

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.

Внимание! Ваш E-Mail будет заблокирован!

От кого: "Служба поддержки Mail.Ru" <antispam000456040457@mail.ru>

Кому: [REDACTED]

Сегодня, 0:33 | Важное

От кого: support@corp.ru **адрес администрации @corp.mail.ru**

Кому: <marina@mail.ru>

Дата: 18 Мар 2010 00:48:33

Тема: Активация

Уважаемый пользователь!

Ваш E-Mail попал в чёрный список антиспама компании Mail.ru. Вам необходимо подтвердить, что Ваш E-Mail не используется для рассылки рекламных писем.

Для подтверждения Вашего электронного адреса, необходимо подтвердить регистрацию. В противном случае согласно разделу 14 пункту 14.2 пользователи Администрации Mail.ru оставляет за собой право заблокировать Ваш аккаунт.

Пройти валид

Эти меры принимаются в связи с возросшим количеством спама. Администрация Mail.ru вынуждена ужесточить политику борьбы с ним.

С Уважением Администрации Mail.Ru

Здравствуйте Ув.пользователь.

Ваш аккаунт на сайте Mail.ru подозревается в массовой рассылке спам-сообщений. Для подтверждения того, что Вы не робот, введите заново свои регистрационные данные по ссылке расположенной ниже:

<http://win.mail.ru/cgi-bin/login?>

Если в течении 3-х дней Вы не подтвердите свои данные, мы будем вынуждены заблокировать Ваш аккаунт без возможности восстановить.

С Уважением, администрация Mail.Ru

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

Фишинг:

а) почтовый

б) онлайнный

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.

The image shows a browser window displaying a phishing page for vkontakte.ru. The browser's address bar shows the URL <http://vkontakte.ru/>. The page content includes the vkontakte logo and a login form with fields for 'E-mail или Логин:' and 'Пароль:'. A red arrow points to the address bar, highlighting the URL. The page also features a sidebar with navigation links and a main content area with text and a button labeled 'Вход'.

mail@antispam.mail.ru кому: [redacted] [показать подробные сведения 2:54 \(10 ч. назад\)](#) [Ответить](#)

mail.ru

ВКонтакте | Добро пожаловать

Вконтакте

E-mail или Логин:

Пароль:

Добро пожаловать

ВКонтакте - универсальное средство общения

Мы хотим, чтобы друзья, однокурсники, родные и коллеги могли в удобном и безопасном для собеседника формате общаться друг с другом. Для этого мы создали новую функцию - обмен сообщениями. Теперь вы можете общаться друг с другом в удобном для вас формате - через электронную почту. Для этого достаточно указать свой электронный адрес в настройках профиля. Мы хотим, чтобы друзья, однокурсники, родные и коллеги могли в удобном и безопасном для собеседника формате общаться друг с другом. Для этого мы создали новую функцию - обмен сообщениями. Теперь вы можете общаться друг с другом в удобном для вас формате - через электронную почту. Для этого достаточно указать свой электронный адрес в настройках профиля.

Нас уже **53 142 918**.

ВКонтакте - самый посещаемый сайт в России

С помощью этого сайта Вы можете:

- Найти людей, с которыми вы хотите общаться.
- Узнать больше о людях, которые вас интересуют.
- Всегда оставаться в контакте с друзьями.

ими жалобами на рассылку рекламных писем (спам) с вашего электронного адреса [redacted]@mail.ru, мы решили заблокировать Вашу учетную запись.

Для продолжения использования электронным адресом, Вам необходимо подтвердить, что Ваш электронный адрес не используется для рассылки рекламных писем.

Внимание, после третьего извещения Ваша учетная запись будет удалена. Все письма, отправленные на этот адрес будут переданы обратно отправителю.

Для подтверждения электронного адреса [redacted]@mail.ru, заполните форму ниже:

http://r2.mail.ru/clb_win.mail.ru/win.rmail.ru/_cgi-bin/

Для подтверждения электронного адреса, авторизовавшись на сервере [redacted]

В течение суток Вам будет выслано письмо с инструкциями как защитить свой электронный адрес от спама. Для получения информации о спонденции. Чтобы подробнее узнать об услуге — посетите [Corp.Mail.Ru](#)

В связи с возросшим количеством нежелательных писем, получаемых пользователями @mail.ru, мы решили ужесточить политику борьбы со спамом. Приносим свои извинения.

www.vkontakte-x.ru

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

Фарминг

Способы минимизации рисков

- 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

M 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 Екрота 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,

gibemem

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

«Нигерийские письма»

Способы минимизации рисков

- 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

3

Вы просите перевести деньги

5

К вам приходит письмо, похожее на PayPal

6

Вы отправляете товар и вводите номер отправления в указанную в письме страницу

2

Мошенник высылает Вам письмо с предложением купить товар, иногда за большую цену и не для себя

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



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 англ. 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

РАММ-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.

The collage displays several screenshots of investment websites:

- HourlyPayment.org:** Features a navigation bar with 'Главная', 'Новости', 'Вопрос-ответ', and 'Форумы и мониторинги'. The main heading is 'надёжные ВКЛАДЫ'.
- FRESH-INVEST.COM:** Promotes a 'ЛУЧШИЙ ИНВЕСТИЦИОННЫЙ ПРОЕКТ' with a '50% за 24 часа' return. It lists features: 'ВКЛАДЫ ОТ 10 ДО 15000 РУБ.', 'ЕЖЕДНЕВНЫЕ ВЫПЛАТЫ', '+50% К ВКЛАДУ ЗА 24 ЧАСА', and 'РЕФЕРАЛЬНЫЙ БОНУС 10%'. It also shows a 'ВХОД В АККАУНТ' section with login and registration options.
- Семьцветик:** A 'Касса финансовой взаимопомощи' with a navigation bar including 'Главная', 'О проекте', 'Правила', 'FAQ', 'ОИИ', and 'Видео'. The main text asks 'Мечтаешь разбогатеть? не упусти возможность' and features an image of a woman with a money bag.
- Statistical Dashboard:** A section titled 'ВАША СТАТИСТИКА' showing 'Активные вклады: 40.00 \$', 'Все вклады: 40.00 \$', 'Сумма выплат: 255000.00 \$', 'Ваши рефералы: 0', and 'Активные рефералы: 0'. Below it is a 'ВЫПЛАТЫ' table listing users and their amounts.

Формы мошенничества и способы минимизации рисков

III. Кибермошенничество

Хайп

Способы минимизации рисков

- 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 домуншники

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

a) 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
использовани
ем 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, наклейки в местах ввода PIN-кода и



Формы мошенничества и способы минимизации рисков



II. Мошенничество
с использованием
банковских карт

Способы минимизации рисков

б) online:

- интернет-мошенничества

- 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 «вспомогательный» чип слетел

до 30 дней.

При использовании банкоматом проявлять осторожность, обращать внимание на

V. Другие виды финансового мошенничества

брачные аферы

нелегальные азартные
игры

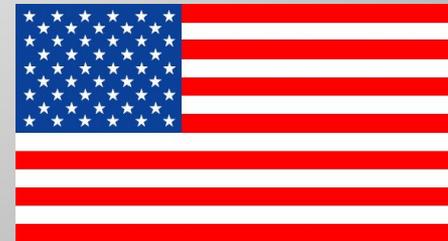
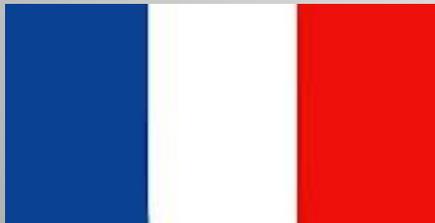
раздолжники

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.