Федеральный проект «Содействие повышению уровня финансовой грамотности и развитию финансового образования в Российской Федерации»

ФИНАНСОВОЕ МОШЕННИЧЕСТВО И РИСКИ ФИНАНСОВЫХ ПИРАМИД

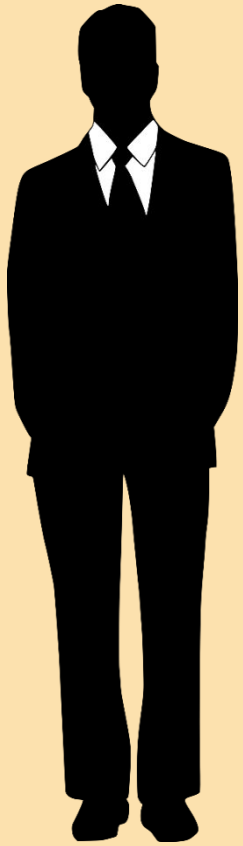
ФИНАНСОВАЯ ГРАМОТНОСТЬ -

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

Что значит «финансово грамотный человек»?

- Планирует свое благополучие
- Определяет финансовые цели и их приоритеты
- Ведет учет расходов и доходов
- Живет по средствам
- Минимизирует долги
- Формирует резервный фонд на неопределенные расходы
- Разумно инвестирует и приумножает капитал



- Пользуется услугами финансовых консультантов
- Разбирается в финансовых инструментах, получает актуальную информацию и новые знание
- Учится сам и передает свои знания семье, детям, близким
- Осознанно выбирает услуги финансовых партнеров и строит долгосрочные доверительные отношения с финансовыми институтами
- Планирует жизнь на пенсии, имеет пенсионный план

Финансовая грамотность – навык использования продуктов, услуг и «законов» финансовой системы себе во благо

«Финансово безграмотный человек»

- Дополнительные риски;
- Низкий уровень финансовой безопасности.

Именно на такого человека легче воздействовать основными приемами деятельности мошенников :

- **информационно-психологическое воздействие;**
- **активная рекламная деятельность.**

Финансовая безграмотность – угроза личной финансовой безопасности

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

ПРЕДПОСЫЛКИ ВОЗНИКНОВЕНИЯ ФИНАНСОВОГО МОШЕННИЧЕСТВА В СОВРЕМЕННОМ МИРЕ

- ✔ увеличение объема финансовых транзакций у каждого из нас;
- ✔ снижение возраста участников товарно-денежных и иных видов сделок;
- ✔ разнообразие видов денег и ценных бумаг;
- ✔ повышение доступности и конфиденциальности персональных данных;
- ✔ увеличение объема сделок вне личного контакта участников (интернет-торговля);
- ✔ исчезновение границ для свободного перемещения денег, товаров, услуг в процессе глобализации (рост транснациональной финансовой преступности);

ПРЕДПОСЫЛКИ ВОЗНИКНОВЕНИЯ ФИНАНСОВОГО МОШЕННИЧЕСТВА В СОВРЕМЕННОМ МИРЕ

- ✔ резкое ускорение процессов технологизации нашей жизни ;
- ✔ отставание технологий защиты функционирования финансовых систем всех уровней перед кибермошенниками;
- ✔ поведенческий и интеллектуальный разрыв между организаторами мошеннических схем и другими участниками финансовых отношений;
- ✔ сверхвысокие доходы участников финансовых афер при весьма умеренном наказании в большинстве стран мира;
- ✔несоответствие поведенческих стереотипов участников финансово-денежных отношений новому уровню рисков.

ПРИЧИНЫ МОШЕННИЧЕСТВА В РОССИИ:

- духовный кризис общества
- обострение социальных противоречий
- рост уровня бедности
- неэффективная система борьбы с преступностью
- правовой вакуум
- правовой нигилизм

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.

Статистика

В 2015 году в России было совершено 38 тысяч преступлений мошеннического характера с использованием средств мобильной связи. Рост по сравнению с 2014 г. – более чем на 50 %.

Ущерб от подобных преступлений в 2015 году составил 1,5 млрд. рублей.

Статистика

По данным Сбербанка годовой ущерб России от киберпреступлений составил

70 млрд. руб.

Ежедневно банк предотвращает кражи на

170-200 млн. руб.

Ежегодные потери мировой экономики от кибератак Всемирный банк оценивает в

445 млрд. долл.

Динамика изменения доли мошеннических операций в общем количестве операций по банковским картам за 2006 - 2011 гг.

payonline.ru

СТАТИСТИКА ЧИСЛА ПРЕСТУПЛЕНИЙ В КРЕДИТНО-ФИНАНСОВОЙ (ЭКОНОМИЧЕСКОЙ) СФЕРЕ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Данные официальной статистики Банка России за 2014-2015 гг.

Совершено более 300 000 несанкционированных операций с использованием платежных карт эмитированными на территории РФ на общую сумму 1,58 млрд рублей.

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

МОШЕННИЧЕСТВО С БАНКОВСКИМИ КАРТАМИ

Практически любое использование банковской карты несет риск возникновения мошенничества (впрочем все операции с наличными денежными средствами тоже нельзя назвать абсолютно надежными).

Основной целью мошенников является получение собственно банковской карты или ее реквизитов, достаточных для совершения мошеннических операций.

Выполнение необходимых мер безопасности позволяет держателю карты пользоваться всеми преимуществами своей карты сводя риски до уровня, равного или ниже рисков расчетов наличными денежными средствами.

ДЛЯ ЧЕГО НУЖНА ПЛАТЕЖНАЯ КАРТА

- Снятие наличных в банкомате;
- Оплата товаров и услуг в магазинах, ресторанах и т.п.;
- Оплата товаров услуг в сети Интернет.

БАНКОВСКИЕ ПЛАТЕЖНЫЕ КАРТЫ(РЕКВИЗИТЫ)

Лицевая сторона банковской карты:

Ни один из реквизитов банковской карты в отдельности не может быть использован для совершения операций

Держатель обязан хранить в секрете:

- реквизиты карты, выделенные на этом слайде зеленым цветом;
- информацию в электронном виде, записанную в микропроцессоре и на магнитной полосе карты;
- PIN-код карты

Лицевая сторона карты:

1,2 - информация банка эмитента и его логотип

3 - микропроцессор - используется при совершении операций в электронных терминалах и банкоматах (практически невозможно скопировать)

4 - номер карты (выдавлено или вырезано на пластике) - используется в сети интернет, переводах с карты на карту

5 - 4 первых цифры номера карты (напечатано)

6 - срок действия карты - используется в сети интернет

7 - имя владельца - используется в сети интернет

8 - логотип платежной системы

В зависимости от видов карт возможны незначительные отклонения в их реквизитах

БАНКОВСКИЕ ПЛАТЕЖНЫЕ КАРТЫ(РЕКВИЗИТЫ)

Оборотная сторона банковской карты:

Ни один из реквизитов банковской карты в отдельности не может быть использован для совершения операций

Держатель обязан хранить в секрете:

- реквизиты карты, выделенные на этом слайде зеленым цветом;
- информацию в электронном виде, записанную в микропроцессоре и на магнитной полосе карты;
- PIN-код карты

Оборотная сторона карты:

1 - телефон горячей линии банка(рекомендуется записать в телефон или блокнот и иметь при себе на случай утери или кражи карты)

2 - магнитная полоса используется при совершении операций в электронных терминалах и банкоматах (копируется очень легко)

4 - 4 последних цифры номера карты (напечатано)

5 - секретный код для использования в сети интернет

6 - образец подписи держателя - используется при совершении операций в торговых точках без использования PIN-кода

7 - голограмма платежной системы

8 - официальные информация о банке эмитенте

В зависимости от видов карт возможны незначительные отклонения в реквизитах

ОБЩИЕ ПРАВИЛА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ БАНКОВСКОЙ ПЛАТЕЖНОЙ КАРТЫ:

- При получении карты в банке убедитесь, что конверт с ПИН-кодом не поврежден.
- НИКОМУ не сообщайте свой ПИН-код (в том числе родственникам или сотрудникам банка).
- Никогда не передавайте банковскую карту для использования третьим лицам, в том числе родственникам.
- Запомните свой ПИН-код. Никогда не храните ПИН-код рядом с картой.
- Если Вы потеряли карту – НЕМЕДЛЕННО свяжитесь с банком и заблокируйте её.
- Регулярно проверяйте выписку по счету.
- Не отвечайте на электронные письма или СМС, в которых от имени банка просят сообщить свои персональные данные или данные карты.

Мошенничество посредством скимминга

Скимминг – наиболее распространенный вид мошенничества, направленный на получение данных о банковской карте (как правило копии магнитной полосы и PIN-кода) для последующего изготовления поддельной банковской карты и использования ее для снятия денежных средств. Реализуется путем установки дополнительной аппаратуры (скиммеров) на действующие устройства самообслуживания, или фальшпанелей устройств самообслуживания.

Мошенничество с помощью «скиммеров»

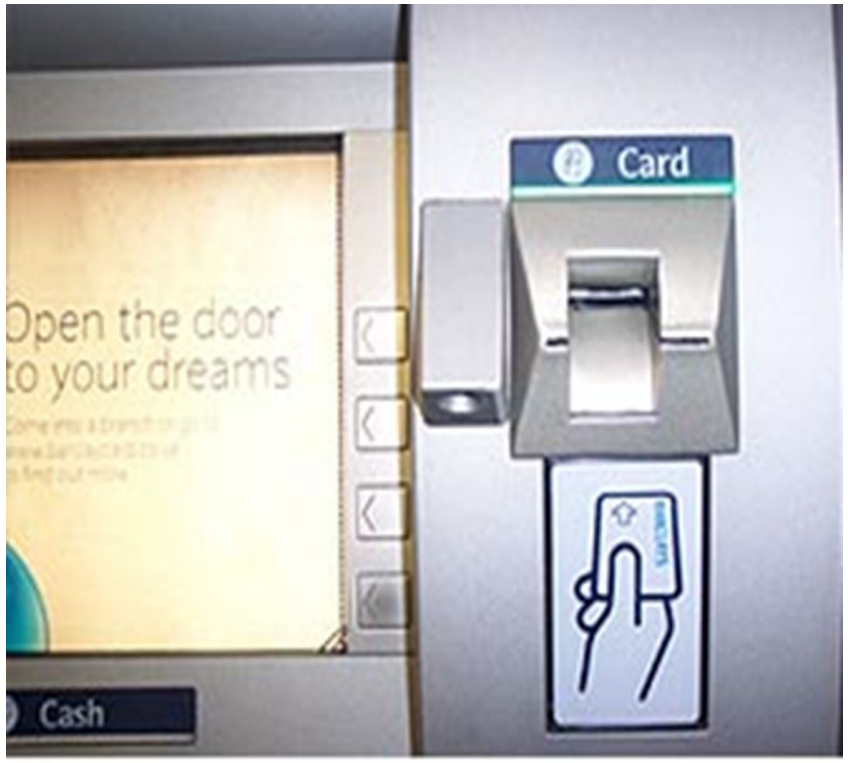
Скиммер – это специальное накладное устройство для банкомата, которое считывает номер вашей банковской карты.

- размером это устройство с пачку сигарет;
- накладывается непосредственно на картридер, в который вы вставляете свою карту.

Мошенничество с помощью «скиммеров»

Так выглядит
«чистый» банкомат:

Так выглядит
банкомат со скиммером:



Мошенничество с помощью «скиммеров»

Схема махинации проста: Вы совершаете любую операцию с помощью банкомата и, ничего не подозревая, уходите по своим делам. В то время как мошенники с помощью скиммера считали всю информацию о вашей карте, в любой момент сделают её дубликат и обнулят ваш банковский счет.

Откуда же они узнают пин-код?

Здесь есть несколько вариантов:

- самый элементарный – человек, стоящий за вами в очереди просто подсмотрит пин-код из-за вашей спины;
- Мошенники могут распылить на клавиатуру специальный спрей, на котором будут четко видны нажатые вами клавиши;
- Мошенники могут установить накладную клавиатуру, которая почти ничем не отличается от самой клавиатуры банкомата;
- Установка на банкомат микрокамеры, и вы её не заметите, потому что спрятана она будет за пачкой рекламных буклетов.

Мошенничество с помощью «скиммеров»

Борьба со «скиммерами»

– ведение видеонаблюдения за банкоматами, использование специальной сенсорной сигнализации;

– установка антискиммеров – специальных накладок на картридер, которые делают невозможным установку скиммера.

Мошенничество с помощью «ливанской петли»

Ливанская петля – приспособление для удерживания банковской карты в устройстве самообслуживания и последующего ее извлечения злоумышленником.

Целью данной махинации является овладение вашей банковской картой.

И если в предыдущих способах мошенникам нужно было иметь специальные устройства, то в этом случае нужна лишь обычная фотопленка.

Мошенничество с помощью «ливанской петли»

- Мошенник изготавливает из фотопленки специальный карман, который помещает в картридер. Концы кармана незаметно закрепляет снаружи картридера.

- Вы решили снять деньги, вставили в банкомат карту, ввели пин-код, и возможно даже обналичили некоторую сумму. Только банкомат возвращать карту вам не стал.

- Вы в панике. «Добрый» человек из очереди вызывается вам помочь, мотивируя тем, что с ним такое тоже случалось. Он нажимает какие-то кнопки, успокаивает вас, а, по сути, через минуту-две вы невольно сообщаете ему пин-код. Извлечь карту никак не получается, и вы (по совету того же «доброго человека») сломя голову бежите в банк разбираться. Или звоните, но вам говорят, что карту извлекут лишь в конце дня при инкассации.

- Вы уходите прочь и ждете звонка из банка. В то время мошенник извлекает петлю и забирает вашу банковскую карту. Сами понимаете, ничего копировать ему не нужно – у него есть оригинал карты и ваш пин. Можете считать, что денег на вашем счету больше нет.

Банковские платежные карты (банкомат)

При использовании банковской карты в банкоматах и других устройствах самообслуживания:

1. До совершения операции необходимо убедиться, что за Вами никто не подсматривает, при вводе ПИН-кода клавиатуру необходимо прикрывать рукой
2. До совершения операции необходимо по возможности убедиться в отсутствии на банкомате посторонних устройств, предназначенных для копирования реквизитов или электронных данных с карты
3. При совершении операций по карте в банкомате нельзя доверять советам третьих лиц и прибегать к помощи посторонних
4. Осуществляйте операции с использованием банкоматов, установленных в безопасных местах (например: в офисах банков, крупных торговых комплексах, государственных учреждениях)
5. В случае задержания банковской карты устройством самообслуживания позвоните в свой банк по горячей линии и следуйте полученным указаниям.

Банковские платежные карты (оплата товаров)

При использовании банковской карты в торговой точке, ресторане и пр.:

1. Требуйте проведения операций с платежной картой только в Вашем присутствии
2. До подтверждения операции с помощью PIN-кода убедитесь в правильности суммы операции на экране устройства
3. Перед тем, как ввести ПИН-код убедитесь в том, что находящиеся в непосредственной близости люди, не смогут его увидеть, либо прикрывайте ввод ПИН-кода рукой
4. Пользуйтесь услугой моментального оповещения об операциях с картой (смс-информирование).

Основным риском является риск компрометации банковской карты или ее реквизитов и последующее использование данных для совершения мошеннических операций как правило в сети интернет.

Банковские платежные карты (интернет)

При использовании банковской карты в интернет-магазинах:
1. Необходимо установить на свой компьютер антивирусное. программное обеспечение, регулярно проводить его обновление и обновление других используемых программных продуктов (операционной системы и прикладных программ).
2. Если Вы пользуетесь неизвестными ранее интернет-магазинами, то имеет смысл открыть для этого специальную платежную карту, на которой в каждый момент времени будет только необходимая для совершения операции сумма.
3. Убедитесь, что Вы находитесь именно на сайте нужного Вам интернет-магазина, сверив информацию в адресной строке браузера или сертификат узла сети (имя ложного сайта может быть очень похожим на имя оригинала).
4. По возможности пользуйтесь картой только на сайтах, поддерживающих защищенный режим обмена данными, о чем свидетельствует наличие префикса *https* в адресной строке браузера и замочек в строке состояния браузера.
5. По возможности выбирайте для использования карты банков, поддерживающих технологии 3D-Secure, что значительно уменьшает риск совершения мошеннических операций и увеличивает шансы на возврат несанкционированно списанных сумм.
6. Заказывая товары и услуги в сети Интернет, не следует сообщать и вводить ПИН-код.

ПРАВИЛА БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ

1. Давая согласие банку на получение карты по почте и на ее активацию по телефону, вы рискуете потерей денег, т.к. при не личной передаче карты она может попасть в руки третьих лиц.

2. Подписывайте карту на обратной стороне, обращая внимание на соответствие подписи с той, что зафиксирована в паспорте.
3. Необходимо хранить номер карты и пин-код в тайне от вторых и третьих лиц.

4. Также ни при каких условиях никому (даже представителю банка) не давайте пароль доступа к своему счету через интернет.

5. Оформите услугу SMS-оповещения о проведенных операциях по карте.

ПРАВИЛА БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ БАНКОВСКИХ КАРТ

6. Услугу по предоставлению овердрафта лучше заключать отдельным договором с банком – в таком случае меньше вероятность просмотреть те условия, которые обычно пишутся мелким шрифтом.

7. Уничтожайте копии чеков, билетов и других документов, где указан номер Вашей карты. Эти данные могут открыть мошенникам доступ к вашим деньгам.

8. Старайтесь по возможности никогда не передавайте (и не показывайте!) банковскую карту для использования третьим лицам.

9. При утере/хищении карты немедленно заблокируйте ее.

Осматривайте банкомат перед его использованием на предмет обнаружения устройств, которые ранее Вами не наблюдались.

10. Старайтесь пользоваться только банкоматами, установленными в безопасных местах.

11. При вводе пин-кода не стесняйтесь закрывать клавиатуру.

ФЕДЕРАЛЬНЫЙ ЗАКОН

С 01.01.2014 года вступили в действие положения статьи 9 Федерального закона от 27.06.2011 №161-ФЗ «О национальной платежной системе», в соответствии с которыми:

1.Банк обязан информировать клиентов обо всех операциях, совершенных с ЭСП, в т.ч. с банковской картой. Способ информирования определяется договором между банком и клиентом.

2.Клиент обязан предоставить банку контактную информацию для обеспечения возможности направления уведомлений, а в случае ее изменения - незамедлительно информировать кредитную организацию. В противном случае банк вправе отказать клиенту в выдаче ЭСП.

3.В случае совершения несанкционированной операции, клиент должен для возврата средств по ней сообщить об этом в банк не позднее следующего дня после получения уведомления от банка. Банк обязан вернуть эти средства, если не докажет, что имело место нарушение клиентом условий договора.

ФЕДЕРАЛЬНЫЙ ЗАКОН (ПРОДОЛЖЕНИЕ)

Для сокращения рисков мошенничества с Вашей платежной картой при ее активном использовании и обеспечения возврата незаконно списанных средств рекомендуется:

- подключиться к системе SMS-информирования банка для как можно быстрого получения информации обо всех совершенных операциях;
- контролировать операции по счету банковской карты по выписке, которую банк Вам предоставит установленным в договоре способом;
- при получении информации об операции, которую Вы не совершали, немедленно сообщить об этом в банк по контактному телефону, указанному на оборотной стороне карты и не позднее следующего дня после получения уведомления о несанкционированной операции следует обратится в банк-эмитент с письменным заявлением о возврате средств.

Внимательно читайте условия заключаемого договора с банком и прилагающиеся к нему правила и/или условия использования банковской карты, так как при возникновении спорных ситуаций банк будет руководствовать условиями договора.

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

Мошенничество с помощью «фишинга»

Фишинг – чаще всего подстановка ложного сайта мошенников вместо сайта интернет-магазина с целью получить введенные клиентом для совершения операции реквизиты карты с их дальнейшим использованием злоумышленниками как правило в сети интернет.

Перехват информации о реквизитах карты при их передаче с Вашего компьютера на компьютер интернет-магазина с дальнейшим их использованием для совершения мошеннических операций как правило в сети интернет.

Мошенничество с помощью «фишинга»

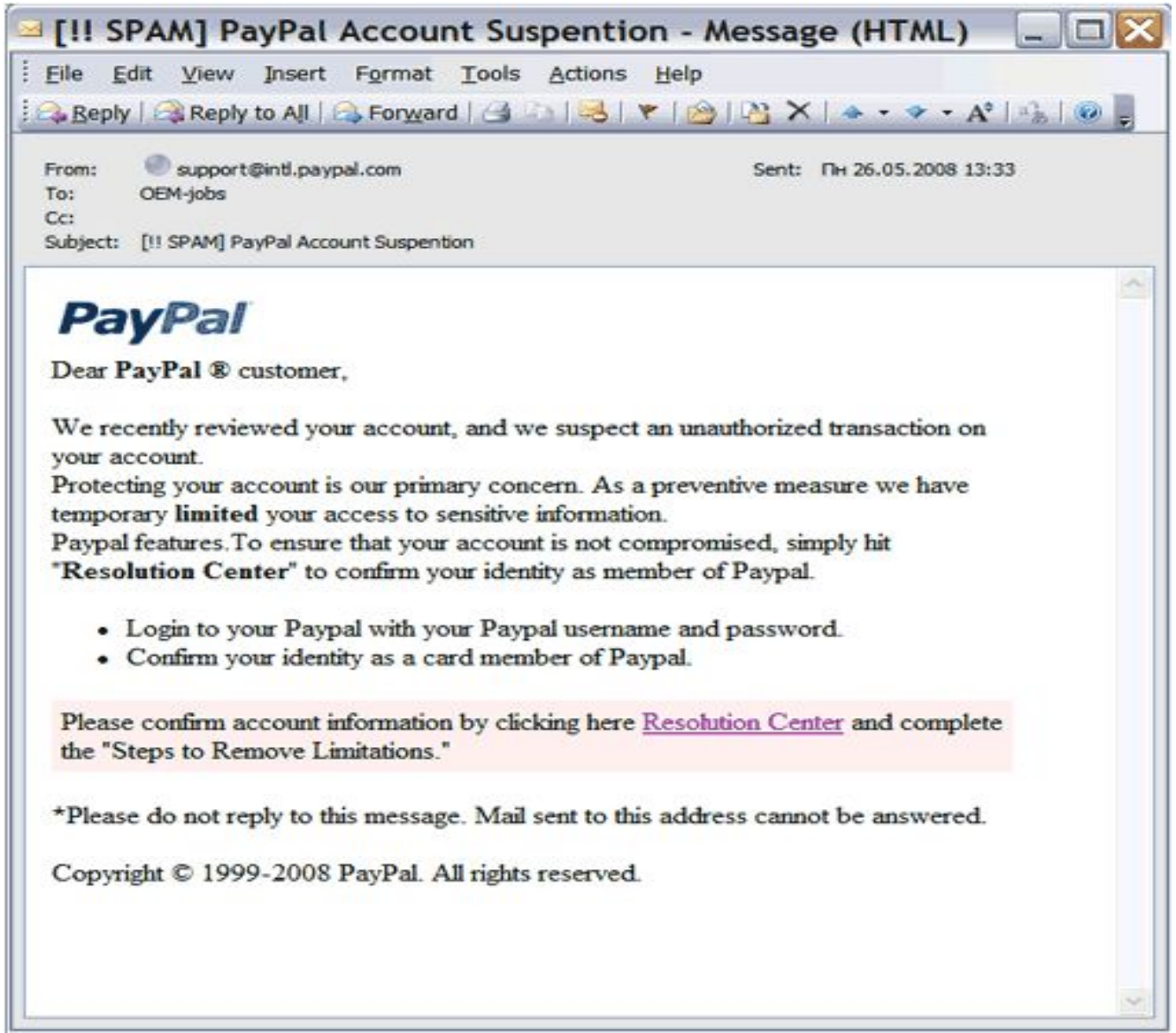
Фишинг (англ. *phishing*) – измененная форма от английских слов «phone» (телефон) и «fishing» (рыбная ловля).

Термин появился для обозначения новых схем, в результате которых путем обмана мошенникам становятся доступны реквизиты банковской карты, секретные пароли для входа и совершения операций в интернет-банкинге или Ваша карта оказывается подключенной к мобильному банкингу на телефон мошенников и т.п.

Чаще всего используется в виде рассылки писем через Интернет или через SMS через телефон от имени банка или платежной системы с просьбой подтвердить конфиденциальную информацию на сайте организации или по телефону, совершить какие либо манипуляции на банкомате и т.п.

В случае получения фишингового письма или SMS игнорируйте подобные сообщения. Перезванивайте в свой банк только по официальным номерам телефонов, указанным на Вашей карте.

Образец фишингового письма



[!! SPAM] PayPal Account Suspention - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply | Reply to All | Forward

From: support@intl.paypal.com Sent: Пн 26.05.2008 13:33
To: OEM-jobs
Cc:
Subject: [!! SPAM] PayPal Account Suspention

PayPal

Dear **PayPal ®** customer,

We recently reviewed your account, and we suspect an unauthorized transaction on your account.
Protecting your account is our primary concern. As a preventive measure we have temporary **limited** your access to sensitive information.
Paypal features.To ensure that your account is not compromised, simply hit "**Resolution Center**" to confirm your identity as member of Paypal.

- Login to your Paypal with your Paypal username and password.
- Confirm your identity as a card member of Paypal.

Please confirm account information by clicking here Resolution Center and complete the "Steps to Remove Limitations."

*Please do not reply to this message. Mail sent to this address cannot be answered.

Copyright © 1999-2008 PayPal. All rights reserved.

Нигерийские письма счастья

Данный вид мошенничества именуют «нигерийским» или «аферой 419» потому, что первые подобные послания - еще в виде обычных писем – стали поступать именно из Нигерии.
Номер 419 – номер соответствующей статьи законодательства данной страны.
С появлением интернета мошенники переключились на электронные рассылки

Нигерийские письма счастья

Мошенники рассылают письма, в которых, как правило, просят помощи в обналичивании солидной суммы в несколько миллионов долларов и предлагают адресату разделить случайно попавшие к ним деньги или солидное наследство.

Для успешного проведения операции от посредника или наследника требуются незначительные (по сравнению с предстоящими доходами) деньги.

Злоумышленники готовы предоставить своей потенциальной жертве отсканированные документы, заручиться со словом адвоката или, на худой конец, почтенного пастора, который подтвердит правдивость рассказанной в письме истории.

Пример

Меня зовут Бакаре Тунде, я брат первого нигерийского космонавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским космонавтом, который отправился с секретной миссией на советскую станцию «Салют-6» в далеком 1979 году. Позднее он принял участие в полете советского «Союза Т-16З» к секретной советской космической станции «Салют-8Т». В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли «Прогресс» снабжают его необходимым. Несмотря ни на что, мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата составила 15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем оплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами. Вечно ваш, доктор Бакаре Тунде,

Формы мошенничества и способы минимизации рисков

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

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

Кибермошенничество

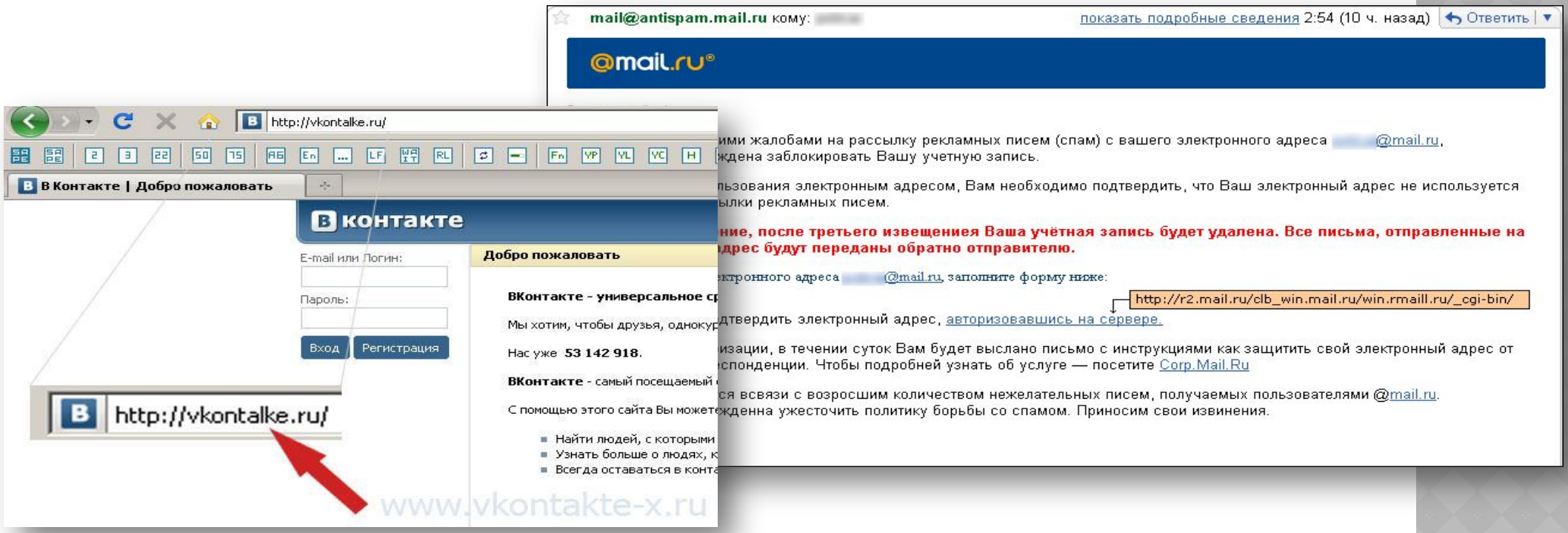
- Вишинг
- Смишинг

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

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

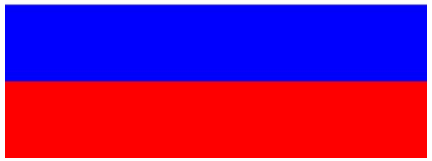
Другие виды финансового мошенничества

Финансовое мошенничество	Способы минимизации рисков
- обмен валюты	- совершать валютно-обменные операции в банках; - минимизировать данные операции в обменных пунктах; - быть внимательным, так как курс может быть указан без учета комиссии, либо выгодным он является исключительно при обмене очень больших сумм; -всегда пересчитывать денежную сумму.
- нелегальные кредиты	- изучить официальную информацию о компании (реквизиты, юридический и фактический адрес) ; - проверить наличие информации о финансовой компании на сайте надзорного органа – ЦБ РФ; - посмотреть отзывы о компании в независимых блогах и социальных сетях.

Современные тенденции в кибермошенничестве

Социальное манипулирование (социальная инженерия) это метод управления действиями человека, основанный на использовании его слабостей и индивидуальных особенностей.

Техническая и технологическая инфраструктура используется только для обеспечения контакта.

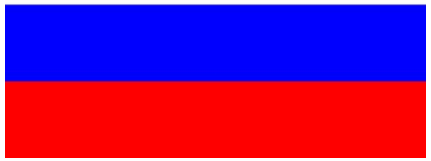


Современный опыт законодательной борьбы с финансовым мошенничеством

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

КРЕДИТ НА ЧУЖОЕ ИМЯ

Оформление кредита на чужое имя — это новый распространённый вид мошенничества. Преступнику достаточно знать ваши паспортные данные и создать поддельный документ с теми же данными и собственной фотографией. После этого он идёт в отделение банка, оформляет кредит на ваше имя, получает в кассе деньги и скрывается. А вы через несколько месяцев получаете звонок из банка с просьбой погасить проценты.

Чтобы не оказаться в подобной ситуации, вы можете сделать следующее:

– Не предоставлять свои паспортные данные непроверенным организациям, особенно если вас просят переслать их через Интернет или в sms/mms и вы ни разу не имели дела с данной организацией лично (sms о выигрыше приза, для получения необходимо прислать фотографию своего паспорта).

– Если вы потеряли (или у вас украли) паспорт, заявите об этом в полицию. Тогда его объявят в розыск и оповестят об этом банки.

– Если на ваше имя всё-таки взяли кредит мошенники, первым делом сообщите банку, что вы такого кредита не брали. Банк может проверить это с помощью графологической экспертизы (сверки подписей на контракте и в вашем паспорте) или посмотрев запись с камер видеонаблюдения, где вместо вас в отделение приходил другой человек.

– Если банк продолжает настаивать на том, что кредит брали именно вы, обратитесь в полицию.

КУДА ЗАЯВИТЬ О СЛУЧАЕ ФИНАНСОВОГО МОШЕННИЧЕСТВА

Вы можете:

- сообщить о подозрительном поведении финансовой организации в местное отделение полиции

- оставить заявку на Правоохранительном портале МВД РФ (www.112.ru) в разделе «Срочная связь» — «Приём обращений» или на сайте Роспотребнадзора (rospotrebnadzor.ru/virtual/feedback/).

КАК РАСПОЗНАТЬ МОШЕННИКА?

- Предложение **сверхвыгодных условий** сделки.
- Необходимость **быстрого** принятия решения.
- Форма общения – панибратство.
- **Демонстративная** роскошь и интеллект.
- Исполнение роли «**важного человека**».
- Предоставление **копий** документов, подтверждающих реальность и надежность компании.

ФИНАНСОВЫЕ ПИРАМИДЫ

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

Финансовая пирамида работает по следующему принципу: организаторы пирамиды собирают у вкладчиков деньги (продают ценные бумаги пирамиды), но не вкладывают эти деньги в экономику, а оставляют у себя. Они объявляют о росте курса своих ценных бумаг, и, когда старые вкладчики

ПРИЗНАКИ ФИНАНСОВОЙ ПИРАМИДЫ

ВАРИАНТЫ РЫНОЧНОГО ПОЗИЦИОНИРОВАНИЯ ФИНАНСОВЫХ ПИРАМИД

проекты не скрывающие, что они являются финансовыми пирамидами

псевдопрофессиональные участники фондового рынка

финансовые пирамиды, позиционирующие себя как альтернатива потребительскому и ипотечному кредиту

проекты работающие под видом микрофинансовых организаций, кредитно-потребительских кооперативов и ломбардов

товарные, сберегательные, туристические и строительные пирамиды

элитные закрытые клубы

Пирамиды обычно обещают сверхвысокую доходность: 200—300 %, а иногда и 1000 % в год. Так как поначалу число вкладчиков всё время растёт, организаторы пирамиды могут какое-то время поддерживать её платёжеспособность. Например, в первый месяц бумаги пирамиды купили 1000 человек. За месяц её бумаги выросли на 50 %. В следующем месяце к пирамиде присоединились ещё 2000 вкладчиков. Даже если все старые 1000 вкладчиков захотят забрать через месяц свои деньги, у пирамиды будет чем с ними расплатиться. 2000 новых вкладчиков принесут в казну пирамиды больше, чем взнос 1000 старых вкладчиков, умноженный на 1,5.

Опасность пирамиды заключается в том, что рано или поздно она рухнет. Слишком много вкладчиков одновременно захотят продать свои ценные бумаги. Организаторы пирамиды поймут, что расплатиться со всеми не получится, приостановят выплаты, а потом скроются с оставшимися деньгами. Конечно, есть шанс, что вы снимете деньги раньше, чем это произойдёт, и тогда пирамида приумножит ваши средства. Но вероятность такого исхода очень низкая. Обычно человек, окрылённый мечтой быстро разбогатеть, несёт деньги в пирамиду снова и снова и попадает на крючок.

- пирамиды обещают очень высокую доходность — сотни процентов в год
- создатели пирамиды обычно не могут подробно объяснить, куда идут деньги вкладчиков и откуда их организация получает доходы.

ВАЖНО:

Помните, что удвоить или утроить свой капитал за 1 год невозможно (если вы не вкладываете его в собственный бизнес, являясь при этом очень удачливым предпринимателем). В погоне за сказочно высокими процентами вы рискуете остаться ни с чем.

Виды финансовых пирамид

1. Схема Понци (Ponzi scheme)

2. Классическая (многоуровневая) пирамида

Схема Понци
(Ponzi scheme)

Ч. Понци, первый пирамидостроитель (бостонский клерк, 1919 г – первая схема Понци)

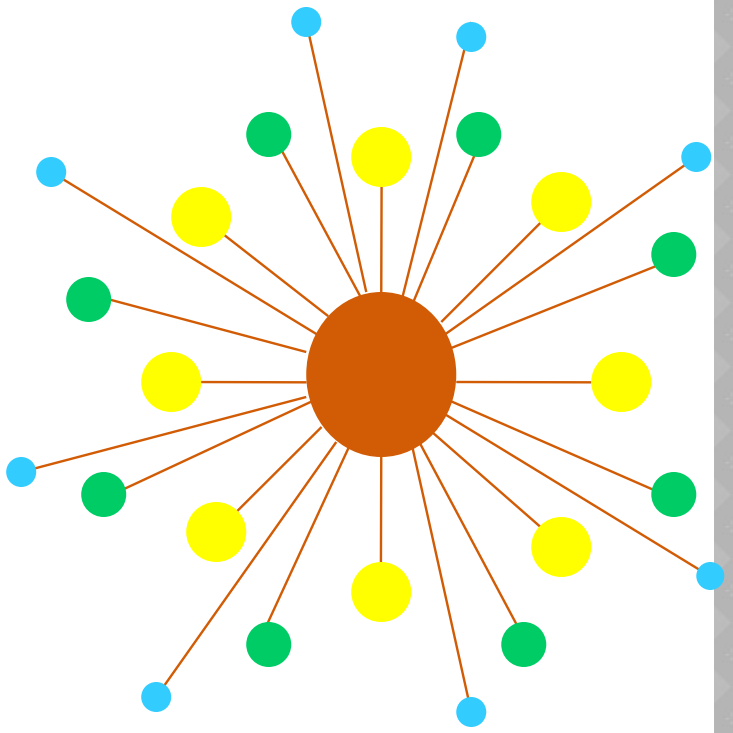


Схема Понци

СХЕМА ПОНЦИ

Схема Понци похожа на финансовую пирамиду тем, что обе они основаны на использовании средств новых инвесторов для финансирования обещанного более ранним инвесторам дохода. Одно из различий между двумя схемами в том, что в схеме Понци, управляющий собирает все соответствующие средства от новых инвесторов, а затем распределяет их. В финансовой пирамиде каждый инвестор непосредственно получает доход от новых инвесторов, в зависимости от того, сколько новых людей становятся новыми инветорами. В этом случае управляющий на вершине пирамиды не имеет доступа к деньгам всей построенной системы.
В обоих случаях, эти схемы обречены на банкротство из-за нехватки денег для выплат.

- иногда начинаются как законный
- бизнес становится схемой Понци, если он продолжает функционировать на мошеннических условиях
- какой бы ни была исходная ситуация, высокая доходность требует возрастающего потока денежных средств от новых инвесторов для поддержания схемы.

Первая финансовая пирамида в СССР

Первые финансовые пирамиды появились на закате истории СССР.

Первооснователем пирамидостроительства в СССР считается фирма «Пакс», созданная в 1991 г. (Волгоград)

Деятельность:
3 года

Похищено:
2 356 960 000 руб.

Обмануто:
1 722 чел.

ФИНАНСОВУЮ ПИРАМИДУ МОЖНО ЗАПОДОЗРИТЬ, ЕСЛИ ИМЕЕТ МЕСТО:

- Массированная реклама.
- Сокрытие подробностей деятельности.
- Малые суммы участия в системе.
- Высокие проценты вложения средств.
- Навязчивая агитация и убеждение.

ПРИЗНАКИ ФИНАНСОВЫХ ПИРАМИД

- Отсутствие лицензии (или указание номера чужой лицензии, или собственной, но выданной на иной вид деятельности)
- Устав не размещен в интернете, а в офисе Вам не хотят его показывать
- Сокрытие финансовой информации (отчеты, балансы…)
- Обещание высокой доходности
- Обещание гарантированных процентов
- Неспособность компании подтвердить свою деятельность

ПРИЗНАКИ ФИНАНСОВЫХ ПИРАМИД

- Подделка под лидера
- Ознакомление клиента с договором только в офисе или при личной встрече
- Упоминание в качестве партнеров хорошо известных фирм
- Требование заплатить вступительный взнос («оформление документов», «участие в семинаре»)
- Место регистрации компании
- Надомная работа
- Спекуляция на насущных потребностях человека
- Давление на психику

Причины, заставляющие людей участвовать в финансовых пирамидах

> 50%

людей сознательно участвуют в финансовых пирамидах с целью заработка

< 50%

людей характеризуются низкой финансовой грамотностью.

Статистика потерь от финансовых пирамид в РФ за 2015 г.

середина 2014 – конец 2015	Доказанный ущерб
250 организаций	2 млрд. рублей.

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

Современные бизнес-модели с элементами финансовых пирамид

Сетевой маркетинг (или многоуровневый маркетинг; англ. *multilevel marketing, MLM*) — концепция реализации товаров и услуг, основанная на создании сети независимых дистрибьюторов (сбытовых агентов), каждый из которых, помимо сбыта продукции, также обладает правом на привлечение партнёров, имеющих аналогичные права.

AVON

MARY KAY

Amway

HERBALIFE

oriflame

natural swedish cosmetics

ОТЛИЧИЯ ПИРАМИДЫ ОТ СЕТЕВОГО МАРКЕТИНГА

Финансовая пирамида	Сетевой маркетинг (Товарная пирамида)
Отсутствие реального продукта	Есть реальная продукция для продвижения на рынке
Высокая стоимость регистрации (500-2000) – необязательно (!)	Бесплатная регистрация или низкая стоимость регистрации (20-50$)
Доход формируется от вступительных взносов привлеченных людей	Доход формируется в результате реализации продукции
Отсутствует обучение	Система обучения, личностный рост
Убеждения, зомбирование	Вы самостоятельно решаете вступать в проект или нет
Отсутствует лицензия (или подделка)	Официальная регистрация, продукция сертифицирована