Конкурс
Защита прав потребителей
финансовых услуг

ТЕМОЦЕНТР

# ФИШКИ и УЛОВКИ ФИНАНСОВЫХ МОШЕННИКОВ

## КАК НЕ ПОПАСТЬСЯ НА КРЮЧОК

# Мошенничество

Как только появились деньги… появились люди, желающие их отобрать.

И вариантов «отъема денег» становиться все больше и больше.

**Примеры «кибермошенничества»**

# Варианты мошенничества

- **Списание денег со счета без ведома владельца,**
- **Кража паролей и ПИН-кодов,**
- **Обещание легкого заработка в интернете**
- **Вклады под невероятные проценты**
- **Онлайн-казино**

**— все это виды финансового мошенничества.**

- Мошенники умеют спекулировать на ваших чувствах, обещать золотые горы, маскироваться под сотрудников банков или государственные организации, чтобы выманить деньги**.** Мошенники умеют выманивать деньги онлайн, с помощью звонков и СМС, в социальных сетях и офисах.

- **Как распознать мошенника и что делать, если вас все-таки удалось обмануть?**

# Телефонное мошенничество

**Как это происходит**

- **«Ваш родственник в беде»**

*Мошенники звонят на телефон вечером или ночью, когда человек дезориентирован или напуган внезапным звонком.*

*Как правило пожилым людям.*

*Представляются другом родственника – сына или внука, попавшего в полицию, больницу, аварию или другую беду.*

*А ему – сыну, внуку, брату – срочно нужна помощь, причем в денежном эквиваленте.*

*Пока потерпевший, готовит все сбережения, преступник, а чаще подставное лицо, например, посредник, появляется на пороге.*

- Все спланировано – плохая связь, ночное время, и пожилой человек спросонья не может сориентироваться.
- Потерпевший добровольно отдает деньги в руки чужого человека, благодарит его за помощь, и только потом начинает анализировать ситуацию, звонит мирно отдыхающему родственнику и узнает, что у него все в порядке.

# «Пополнение счета абонентского номера»

- *Текст смс-сообщения примерно одинаков: "Мама, я в беде. Переведи деньги на (номер счета или номер телефона)", "Кинь деньги, потом объясню".*

- *Раскрыть такие мошенничества намного сложнее. Отправлять такие сообщения можно с компьютера, включив рассылку на сотни номеров. Часто мошенники просят небольшие суммы – до 1000 рублей.*

- Потерпевший бежит к терминалу, перечисляет деньги, и только потом понимает, что его обманули.

## «Вы выиграли приз!»

*На мобильный телефон приходит смс-сообщение о выигранном призе. После того, как владелец телефона связывается с автором сообщения, ему сообщают, что необходимо предварительно оплатить сопутствующую услугу или подоходный налог через систему денежных переводов.*

## «Акции» оператора

*Человек получает сообщение об акции, проводимой его мобильным оператором. По условиям "акции", человек до конца недели (месяца, года, жизни) получает возможность осуществлять бесплатные звонки по стране. Для этого ему необходимо всего лишь отослать в службу информационной поддержки (телефоны прилагались) коды нескольких карт оплаты. Естественно, потом выясняется, что оператор рекламных акций не проводил, а карты оплаты пополнили счета мошенников.*

## «Ваша карта заблокирована!»

*На мобильный телефон потерпевшего приходит смс-сообщение примерно такого содержания: "Ваша карта заблокирована. Подробности по телефону…". Доверчивому гражданину, позвонившему на указанный в сообщении телефон, отвечает якобы представитель технической службы или службы безопасности банка (какого – не уточняют), просят срочно передать данные карты, CVV-код, ПИН-код, дабы карту не взломали мошенники, пробившиеся в службу безопасности банка.*

## «Заявка на перевод денежных средств принята!»

*На мобильный телефон потерпевшего приходит смс-сообщение примерно такого содержания: «Платеж на такую-то сумму одобрен, подробности по телефону…". Гражданина, позвонившему на указанный в сообщении телефон, просят подойти к ближайшему банкомату, войти в меню оплаты и набрать ряд цифр.*

# «Ой, я ошибся номером карты...»

## «Уведомление» о зачислении средств

*Вам приходит СМС о зачислении средств (и сообщение похоже на привычное уведомление банка), а затем звонит якобы растяпа, который по ошибке зачислил вам деньги и просит вернуть.*

*Не спешите ничего возвращать. Такая ситуация больше похожа на мошенническую схему: скорее всего, деньги не приходили, СМС — не от вашего банка, а звонил вам злоумышленник.*

*Проверьте состояние вашего счета, закажите выписку в онлайн-банке или позвоните в банк, прежде чем переводить кому-то деньги.*

## «Подтвердите покупку»

*Вам приходит уведомление «Подтвердите покупку» и код, а следом раздается звонок опять же от «рассеянного» человека, который говорит, что по ошибке указал ваш телефонный номер, и просит продиктовать ему код, ни в коем случае не делайте этого. Мошенники пытаются выманить у вас код, чтобы списать с вашего счета деньги или подписать вас на ненужный платный сервис.*

# БУДЬТЕ БДИТЕЛЬНЫ!

Многие схемы мошенничества основаны на вытягивании у владельца карты конфиденциальной информации с использованием различных психологических манипуляций.
Это работает, как в обычной жизни, так и в онлайн.

Люди, думая, что совершают операцию по разблокировке карты или отмене перевода, сами перечисляют все средства со своей карты на чужой абонентский номер или банковский счет, и только потом звонят в банк, узнать, что же случилось.

**Будьте бдительны! Ни один банк не будет рассылать подобные сообщения, а тем более спрашивать реквизиты карты.**

**Поэтому все сообщения и звонки с подобными предупреждениями – всегда мошенничества.**

# Мошенничество с банковскими картами

Чтобы использовать вашу карту в своих целях, мошенникам нужно узнать ее номер, имя владельца, срок действия, номер CVC или CVV. Они могут установить скиммер на банкомат (специальное устройство, которое накладывают на приемник карты в банкомате) и видеокамеру над клавиатурой.

Достаточно один раз воспользоваться таким банкоматом — и ваши деньги могут снять, перевести на несколько счетов и обналичить.


Украсть данные вашей карты могут даже в кафе или магазине. Злоумышленником может оказаться продавец, который получит доступ к вашей карте хотя бы на пять секунд. Сфотографировав вашу карту, он сможет воспользоваться ей для расчетов в интернете.

# Как не попасться

- Перед снятием денег в банкомате осмотрите его. На картоприемнике не должно быть посторонних предметов, клавиатура не должна шататься.
- Набирая ПИН-код, прикрывайте клавиатуру рукой. Делайте это даже во время расчетов картой в кафе.
- Подключите мобильный банк и СМС-уведомления.
- Если совершаете покупки через интернет, никому не сообщайте секретный код для подтверждения операций, который приходит вам по СМС.
- Старайтесь никогда не терять из виду вашу карту.

# Что делать, если вас обокрали

1. Позвоните в банк (номер всегда есть на обороте карты или на главной странице сайта банка),

2. Сообщите о мошеннической операции и заблокируйте карту.

3. Запросите выписку по счету и напишите заявление о несогласии с операцией.

4. Обратитесь с заявлением в отдел полиции по месту жительства или отправьте сообщение в **Управление «К» МВД России**.

# Как защитить себя от мошенников

1. Оплачивайте покупки только на сайтах известных компаний.
2. Для оплаты покупок через Интернет используйте отдельную банковскую карту с ограниченной суммой денег.
3. Старайтесь пользоваться банкоматами в отделениях банка или внутри зданий организаций и учреждений. Если отдельные детали банкомата выглядят подозрительно, не пользуйтесь таким банкоматом.
4. При вводе ПИН-кода всегда прикрывайте клавиатуру рукой, чтобы его не могли подсмотреть посторонние или записать установленные злоумышленниками скрытые камеры.
5. Если денежные средства не были выданы банкоматом, но вы получили СМС-сообщение об их списании, незамедлительно обратитесь в ваш банк.
6. Установите суточный лимит на снятие наличных в банкоматах.
7. Никому и никому не сообщайте ПИН-код и код CVV2/CVC2 своей банковской карты.
8. Никогда не давайте посторонним лицам данные карты, персональные данные и коды, присланные в СМС.
9. Не переводите и не зачисляйте деньги в ответ на просьбы, поступающие с неизвестных номеров.
10. Не набирайте на мобильном устройстве цифровые команды, назначение которых вам неизвестно.

# Мошенничество на финансовых рынках

На рынке Форекс продают и покупают валюту в основном крупные банки. Чтобы обычному человеку выйти на Форекс, нужно заключить договор с посредником, форекс-дилером, и торговать через него.

- **Псевдопрофессиональные форекс-дилеры** активно рекламируют свои услуги по организации торговли на рынке Форекс, рассказывая заманчивые истории, как простые люди «с улицы» заработали состояние, покупая и продавая валюту на рынке Форекс.
- Псевдо-диллеры предлагают удивительно низкие комиссии, различные бонусы (сумма на вашем счете, допустим, удваивается). Вы даже можете заключить с дилером договор через интернет с помощью электронного документооборота и вроде бы выиграть целый миллион!
- Но прибыль вы не получите и вложения потеряете.

# Мошенничество на финансовых рынках

- Не стоит связываться с так называемыми **бинарными опционами**.
- Реклама в интернете сулит вам неслыханную прибыль: откройте счет, делайте ставки на рост или падение валют или акций за определенный период. Если по истечении заявленного времени ваш прогноз оказывается верен, вы получаете внушительный процент прибыли, если вы не угадали — теряете деньги.
- В реальности сегодня в интернете не существует площадок, на которых могут проводиться такие сделки, поэтому все обещания о легком заработке на бинарных опционах — это мошенничество.
- Вы просто потеряете свои деньги.

# Как уберечься от обмана

- Если вы все же решились выйти на рынок Форекс, внимательно изучите закон и «Базовый стандарт совершения операций на финансовом рынке при осуществлении деятельности форекс-дилера».
- Проверьте форекс-дилера, с которым собираетесь работать, — у него обязательно должна быть лицензия. Уточнить, есть ли она, можно в справочнике участников финансового рынка.
- С 1 января 2016 года осуществлять дилерскую деятельность на территории России могут только лицензированные компании, зарегистрированные на территории РФ.
- Если компания зарегистрирована не в России, а в офшорных зонах, насторожитесь: скорее всего, перед вами мошенники.
- А лучше — не рискуйте, а попробуйте начать путь инвестора на фондовой бирже.

**Если вы стали жертвой мошенничества на финансовых рынках.**
Соберите все документы, которые у вас есть: договоры, заключенные с посредником-мошенником, чеки на перевод денег, сделайте скриншоты с сайта — и отправляйтесь в полицию писать заявление.
Сообщите в Банк России, все жалобы рассматриваются.

# Мошеннические организации

- Мошеннические организации маскируются под микрофинансовые организации, компании сетевого маркетинга, инвестиционные компании, онлайн-казино.
  - Они также заявляют о высоких процентах по вкладам и отсутствии рисков, гарантируют доход (что разрешено только для банковских вкладов), просят внести деньги сразу (желательно наличными) и привести друга (иногда за какой-то бонус).

- Финансовой пирамиды.
  - Например, МММ, обещала огромные проценты по вкладам, гарантировала доходность и выплачивала средства за счет денег, внесенных другими вкладчиками. Верхушка этой пирамиды действительно могла заработать, а те, кто стоял на ступенях ниже, теряли свои деньги.

На финансовых пирамидах заработать нельзя: если вы вложите деньги, вы непременно их потеряете.

# Основные признаки финансовой пирамиды

1-й признак

**Гарантирование постоянной высокой доходности (на уровне 15% – 30% - 50%)**

**ВАЖНО ПОНИМАТЬ!**

Гарантированно высокой, тем более постоянной доходности не бывает

2-й признак

**Отсутствие специальных лицензий**

**ВАЖНО ПОНИМАТЬ!**

Для привлечения вкладов у населения необходима лицензия Центрального банка России.

# Основные признаки финансовой пирамиды


3-й признак

**Форма привлечения денежных средств – договор займа**

**ВАЖНО ПОНИМАТЬ!**

Заключение таких договоров никем не контролируется. Договоры могут содержать массу «лазеек», увидеть которые неспециалисту проблематично.

И, главное, в случае банкротства фирмы шансы получить свои деньги назад практически равны нулю.

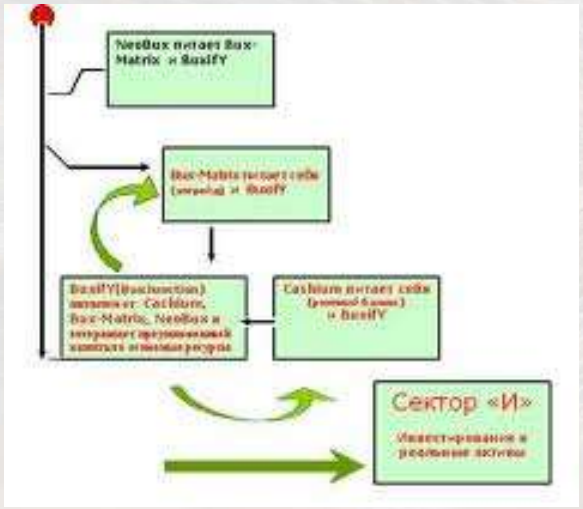
4-й признак

**Выплата вознаграждения за привлечение новых вкладчиков**

# Основные признаки финансовой пирамиды

## 5-й признак
## МАНИПУЛИРОВАНИЕ

- Использование «умных» терминов, с целью создать у слушателя комплекс дилетанта
- Упоминание в качестве «партнеров» известные банки, страховые компании, государственные программы
- Пафосные рекламные кампании, эмоциональное вовлечение




## 6-й признак

**Сложные схемы перемещения вложенных средств**

«Деньги получили в России, застраховали в Швейцарии, акции купили в Америке»

# ПОЛЕЗНАЯ ИНФОРМАЦИЯ

**Служба по защите прав потребителей финансовых услуг и миноритарных акционеров Банка России**
http://www.cbr.ru/
электронная почта: mailto:fps@cbr.ru

**Федеральная антимонопольная служба**
http://www.fas.gov.ru
Электронная почта: delo@fas.gov.ru

**Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор)**
http://rospotrebnadzor.ru

**Финансовый омбудсмен**
Сайт: www.arb.ru.
Электронная почта: finomb@arb.ru

**Генеральная Прокуратура РФ**
http://genproc.gov.ru/