МОДУЛЬ 7.7

Теоретический материал по теме:
«Финансовая безопасность для многодетных семей»

Что такое финансовые риски и от чего нужно защищаться?

Любой человек, у которого есть деньги или имущество, рискует. Предугадать превратности судьбы невозможно, а вот смягчить ее удары, заранее подумать о своей финансовой безопасности и подстраховаться вполне реально.

Финансовая безопасность это про то, как:

- пережить временные финансовые трудности, не меняя привычной для себя жизни;
- избежать участия в сомнительных мероприятиях (финансовых пирамидах) на тему «Как стать богатым в одночасье»;
- защитить свои деньги от потерь, в результате совершения электронных платежей и от мошенников.

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

Существует несколько видов финансовых рисков, угрожающих личным финансам – инвестиционный, инфляционный, валютный, транзакционный и мошенничества.

Есть **два способа** снижения потерь от возможных финансовых рисков:

- формирование *финансового резерва* (финансовой подушки безопасности);

- соблюдение *финансовой гигиены* и выполнение определенных правил.

Финансовый резерв. Правила формирования.

Финансовый резерв (*“заначка” или «подушка безопасности»)* – это накопленный объем денег, позволяющий прожить определенное время при неожиданной потере основного источника дохода или возникновении финансовых трудностей.

Резерв создается не для приумножения денег, а для безопасности, на случаи временных финансовых трудностей, таких как: внезапного увольнения, болезни (в этом случае, будет финансовым резервом и специально оформленная страховка), необходимая дорогостоящая покупка или других сложных ситуаций, из-за которых вы можете потерять доход или вынуждены будете нести крупные траты, или начать что-то новое.

Таким образом, очевидны ПРЕИМУЩЕСТВА ФИНАНСОВОГО РЕЗЕРВА:

- Страховка от непредвиденных обстоятельств.
- Предотвращает появление долгов и необходимости продавать нужное имущество.
- Защита от стресса и источник уверенности в завтрашнем дне.
- Источник стартового капитала при возникновении возможностей.
- Защита от нищеты и полного краха в случае катастрофической ситуации.

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ
ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

БОГАТЕИ С ДЕТСТВА

Создавая финансовый резерв, нужно помнить о важном критерии — возможность быстро получить наличные. Вы также правильно пишете, что для резерва важна защита от инфляции и отсутствие рисков.

Именно отсутствие финансового резерва в момент возникновения сложной ситуации, чаще всего толкает нас на необдуманные поступки, такие, например, как: оформление кредитов, взятие денег в долг. При этом нужно помнить, что бывают такие ситуации, когда сложный период жизни не один, а несколько. И тогда мы понимаем, что создание финансового резерва будет являться неким буфером на пути финансовых угроз.

Как создать финансовый резерв (подушку безопасности)?

Во-первых, посчитать, сколько денежных средств тратит семья в месяц для того, чтобы чувствовать себя комфортно и сильно не ущемлять свои привычки. Можно выбрать другой способ и вместо расходов для определения величины накопления брать размер минимально необходимого дохода на семью в месяц для комфортного проживания. Стоит отметить, что размер финансового резерва каждая семья определяет для себя самостоятельно. Накапливать рекомендуется до тех пор, пока не будет собрана необходимая сумма.

Во-вторых, откладывать рекомендуется часть средств с заработной платы **ежемесячно и** желательно **до или в момент получения дохода**. Здесь будет действовать правило «Сперва заплати себе сам». Кроме того, можно пересмотреть состав своих расходов или найти дополнительные источники доходов, или создать пассивные источники доходов, увеличив размер средств, направляемых в ФР. Хорошо помогает автоматизация процесса формирования и пополнения финансового резерва, т.е. подключите «автоматическую копилку» на своем счете или карте.

В-третьих, накапливать рекомендуется — 10% от дохода семьи. Необходимо акцентировать внимание на том, что не столько важен сам размер, сколько важна регулярность накоплений, так как это формирует финансовые привычки. Почему это важно? Потому что наш с Вами разум всегда найдет 351 причину почему в данном конкретном месяце накопления сделать невозможно. Обычно это как раз тот тип людей, который любит начинать новую жизнь с понедельника, бросает курить и пить со следующего месяца, с нового года начинает заниматься спортом и т.п. Постепенно наращивайте темп и % формирования финансового резерва

В-четвертых, накапливать рекомендуется до тех пор, пока не будет собрана необходимая сумма. Считается, что ФР формируется в размере минимум 3–6-месячных доходов, в зависимости от того, насколько быстро семья сможет восполнить возможность получения регулярного дохода в случае неблагоприятных обстоятельств. Некоторые граждане создают резерв в размере до 36-месячных окладов.

В-пятых, не стоит поддаваться соблазнам и брать из ФР средства на покрытие текущих расходов. Поэтому не стоит хранить ФР (подушку безопасности) дома, где велик соблазн израсходовать деньги по любому «важному поводу»:

1. Усложните доступ к ФР. Не стоит поддаваться соблазнам и брать из ФР средства на покрытие текущих расходов.

2. Планируйте свои расходы заранее, чтобы не выбиваться из бюджета, и как следствие, не прибегать к ФР.

Как видим, ФР (подушка безопасности) не только позволит нам создать резервный фонд и более-менее безболезненно пережить любой финансовый форс-мажор, но и придаст нам чувство уверенности в завтрашнем дне. Большинство людей, по ряду причин с тревогой смотрит в завтра в силу отсутствия стабильности, гарантий и т.п., именно наличие финансовой подушки безопасности поможет нам бороться с этой тревогой (страхами).

Где взять деньги?

Есть два основных варианта: зарабатывать больше или тратить меньше. Лучше всего использовать оба.

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ
ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Какие требования предъявляются к финансовому резерву (подушке безопасности)?

- Неприкосновенность.
- Возможность быстро получить средства.
- Защита от инфляции.

По этим параметрам идеально подходят банковские вклады – деньги можно оперативно снять, начисляется небольшой доход, государство гарантирует возврат средств (вклады застрахованы АСВ — 1,4 миллиона).

Дома можно хранить небольшую часть средств. На всякий непредвиденный случай. Выходные, праздничные дни банки могут не работать, а деньги нужны здесь и сейчас.

Кроме того, хранение средств фонда на депозите позволит получать проценты, и вы сможете увеличивать его объем, капитализируя проценты по вкладу.

Также рассмотрите следующие варианты: накопительные счета, дебетовые карточки с процентом на остаток и/или кэшбеком.

Что точно не нужно делать с деньгами из финансового резерва, так это инвестировать их куда-либо, так как любые инвестиции — это риск. Далеко не факт, что в случае срочной надобности вы сможете вывести свои деньги из инвестиционных проектов без потерь, а именно возможность быстрого доступа и есть одно из основных требований к сбережениям данного типа.

В каких инструментах точно не стоит хранить деньги из финансового резерва:

1. акции, облигации;
2. бытовую технику;
3. недвижимость
4. драгоценные металлы;
5. иностранная валюта.

Недвижимость быстро за один день не продашь, ценные бумаги, могут подешеветь, золото, хоть и считается защитным активом, тоже может снижаться, бытовая техника кроме того, что обесценивается еще и морально устаревает. Поэтому лучше всего хранить финансовый резерв в деньгах.

Следует сделать оговорку в отношении валюты. Считается правильным хранить средства финансовой подушки безопасности в валюте своих расходов. Но памятуя о событиях, когда рубль обесценивался до 40% хранить не только в рублях, но и в другой валюте — долларе и евро. Оптимальным будет соотношение 1:1:1.

Финансовое мошенничество

Мошенничество - «хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием» (ст. 159 УК РФ)

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

Под определение «мошенничество» попадают многие незаконные действия в самых различных сферах, в том числе и в сфере банковской деятельности, сотовой связи и современных информационных технологий. Несмотря на различия в технологии, все эти действия объединяет ряд общих признаков:

- Обманные действия;
- Эмоциональное давление
- Злоупотребление доверием;
- Захваливание, лесть
- Обещание сверхдоходности проекта

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

- Умышленное искажение фактов или умолчание;
- Хищение чужого имущества/вещи;
- Незаконное приобретение прав на чужое имущество/вещь;

В большинстве случаев жертва мошенничества самостоятельно и добровольно передает преступникам свое имущество/вещь

Финансовые пирамиды

Естественно, каждый человек может вкладывать честно заработанные рубли куда угодно: в коробку из-под печенья, кассу взаимопомощи, криптовалюту, кооператив «Рога и копыта», в игру на Форекс. Неотъемлемое право каждого человека – быть обманутым. И несмотря на прошлый опыт (МММ, Властелина и т.п.) мошенники, используя передовые технологии продолжают втягивать нас в сомнительные проекты (финансовые пирамиды) и финансовые сделки.

Из-за жажды легкой наживы, по данным ЦБ в 2018 г. россияне потеряли в финансовых пирамидах более 2,7 млрд. руб.!

В 2019 году Банк России выявил 237 финансовых пирамид, это почти в 1,5 раза больше, чем в 2018 году

С 2016 года в стране действует закон, нацеленный на предупреждение возникновения так финансовых пирамид, предусматривающая административную ответственность за привлечение денежных средств в финансовые пирамиды, а также рекламирование – статья 14.62 КоАП РФ и штраф за подобные действия до 1 млн. рублей. Кроме того, существует и уголовная за организацию финансовых пирамид - статья 172.2 УК РФ. Наказание: штраф до 1 млн. руб до лишения свободы до 4 лет с ограничением свободы). Вместе с тем, не всегда получается привлечь как самих организаторов, так и организации за организацию финансовых пирамид.

Финансовые пирамиды: виды и примеры

За три последних года Центробанк России вычислил порядка 700 организаций, имеющих признаки финансовой пирамиды. Почти 150 из них идентифицированы в 2018 году. Мошенничество подается под разными «соусами», организаторы пирамид могут быть довольно изобретательны. **В 2019 году концепции финансовых пирамид исполнилось 100 лет.**

Среди финансовых пирамид встречаются кредитные потребительские кооперативы, инвестиции в криптовалюты, вложения в облачный майнинг, операции с золотом или просто сетевой маркетинг.

Выделяют **5 основных видов финансовых пирамид**.

1. **Первый вид** – это те проекты, которые и не скрывают, что они финансовые пирамиды. Ярким примером является МММ. Как правило, такие проекты организованы на принципах сетевого маркетинга (multilevel marketing, MLM), когда доход участника (инвестора/вкладчика) формируется за счёт инвестиций/вложений новых привлекаемых им участников.

2**. Второй вид** — финансовые пирамиды, которые позиционируют себя как альтернативу ипотечному и потребительскому кредитованию. Такие структуры рассчитаны на заёмщиков, которым отказали другие финансовые учреждения.

3. **Третий вид** — пирамиды, которые работают под видом микрофинансовых организаций, кредитно-потребительских кооперативов и ломбардов. Чаще всего такие организации привлекают средства от населения в виде займов или путём продажи различных векселей с целью дальнейшей выдачи займов клиентам под более высокий процент. Такие проекты могут существовать в виде виртуальных бирж.

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

4. **Четвёртый вид** — организации, которые предлагают услуги по рефинансированию и софинансированию долгов физлиц перед банками и другими кредитными организациями. По такой схеме компания обязуется погасить все задолженности гражданина перед банком или МФО при условии перечисления ей порядка 30 процентов от суммы взятого кредита или займа. Кстати, такой вид пирамиды является особо опасным, так как когда пирамида рухнет (а она рухнет), то ущерб будет нанесён не только населению, но и финансовым организациям, выдавшим кредиты и займы.

5. **Пятый вид** — «псевдопрофессиональные участники» финансового рынка, которые предлагают услуги по торговле на валютном рынке FOREX.

В чем проявляются современные тенденции в развитии финансовых пирамид?

Хайп проекты. Они действуют исключительно онлайн, а доход «инвесторы» получают за счет новых привлеченных вкладчиков. Мошенникам удобны хайп-проекты: в Интернете можно охватить огромную аудиторию, компания нигде не регистрируется, для нее не надо даже открывать банковский счет. Такие проекты быстро раскручиваются и требуют от организаторов минимального вложения средств»

Загадочное слово "раздолжители". Относительно новый вид финансовых пирамид — так называемые фирмы-"раздолжители". Они обещают решение проблем с кредиторской задолженностью перед банком за вознаграждение. Но переуступки долга по закону не происходит, а гражданин только теряет деньги.

Потребительские эмоции и региональные особенности. Один из самых оригинальных видов финансовых пирамид в России — айфонные. Предприниматель обещает продать дорогой гаджет дешевле на 20–30%, но через три-четыре недели. Клиенты знают, что их друзья уже получили дорогие гаджеты по действительно сниженной цене.

Самым громким скандалом 2018 года явилась ситуация с компанией Кэшбери. Компания, якобы работавшая на рынке микрозаймов, действовала по всей стране на протяжении двух лет, вовлекла в свои сети десятки тысяч человек, нанесла ущерб, по оценке ЦБ, в 3 млрд. рублей. Офисы были открыты во всех крупных городах, в рекламу пирамиды были вовлечены уважаемые СМИ, включая ИД «Коммерсант», «Интерфакс», известные блогеры и медиаперсоны.

В 2019 года такой скандал разразился с двумя компаниями МФК Мани Фани и ООО Смартшеринг.

Что же такое финансовая пирамида?

Это такая мошенническая организация, которая выплачивает своим инвесторам процент с вкладов за счет денежных средств вновь поступающих членов/участников проекта. На слайде вы видите масштабы последствий от участия в подобных организациях/проектах. Последствия участия в финансовых пирамидах грозят большими потерями.

Что нужно знать и как уберечь себя от участия в подобных организациях и последствий?

В первую очередь запомнить основные признаки финансовых пирамид:

- Очень высокая доходность. Процентные ставки по вкладам минимум в 2-3 раза превышают проценты по депозитам в банках.
- Объяснение высокой доходности новыми сверхприбыльными видами инвестирования, которые могут быть не до конца понятны;
- Непрозрачность. Фирма скрывает регистрационные сведения, структуру и состав руководства
- Суперизкие цены. Клиентам обещают продать товары или оказать услуги по цене намного ниже средней рыночной
- Нет лицензии. У компании, которая привлекает вклады, нет банковской лицензии
- Выплаты за счет других клиентов. Клиенты фирмы получают выплаты из средств, которые компания привлекает от других клиентов

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

БОГАТЕЙ С ДЕТСТВА

- Никаких гарантий. Договор составляется таким образом, что клиент ничего не получает в случае краха компании
- Вам предлагают приводить друзей. Фирма предлагает вам приглашать в проект друзей и знакомых, от этого зависит ваш уровень дохода
- Массированная реклама и призывы не раздумывать долго, а быстрее инвестировать деньги;
- Распространение продукта очень похоже на сетевой маркетинг;
- Сокрытие информации о руководстве компании и ее реквизитах, и финансовом положении;
- Требование к инвесторам уплаты регистрационного сбора, зависимость размера прибыли от количества привлеченных клиентов инвестором лично;

Во-вторых, развивать критическое мышление. Задайте себе следующие вопросы: как осуществляется взаимодействие между вами? Каким образом осуществляется денежные операции между мной, компанией, а также другими организациями? Возможно ли забрать денежные средства без потери и в какие сроки? Что вы покупаете за свои деньги?

Как уберечься от участия в таких проектах? Элементарно. Проявляя бдительность:

- Проверьте наличие у финансовой организации лицензии или ее самой в реестре Банка России. Сверьтесь со Справочником по кредитным организациям и Справочником участников финансового рынка.
- Проверьте компанию в Едином государственном реестре юридических лиц ФНС России.
- Запросите образцы договоров, копии документов. Если есть возможность, проконсультируйтесь с юристом.

Но если так случилось, что Вы вложились и прогорели. Что делать?

- Составьте претензию и направьте ее в адрес компании заказным письмом с уведомлением. Или отнесите лично и удостоверьтесь, что его зарегистрировали. Возьмите расписку о получении, чтобы компания якобы случайно не потеряла ваше письмо.
- Если компания отказывается вернуть деньги, то соберите все документы (от договоров до выписок) и обратитесь в правоохранительные органы с заявлением.
- Свяжитесь с юристом и попробуйте найти других жертв мошенничества

Куда писать, если есть подозрение, что вы столкнулись с финансовой пирамидой

- Федеральный общественно-государственный фонд по защите прав вкладчиков и акционеров, их проект СТоп-пирамида: https://stoppiramida.ru/
- Интернет-приемная ЦБ https://cbr.ru/Reception/
- Проект Олега Анисимова Вкладер, он собирает и рассказывает о таких кейсах: https://vklader.com/

К сожалению, финансовые пирамиды не являются исключительным видом, используемым мошенниками. Багаж инструментов, используемых ими широк.

Финансовые риски: Мошенничества при совершении различных финансовых операций, социальная инженерия и прочие «разводы».

К самым распространенным способам мошенничества и наиболее опасным с точки зрения последствий для каждого, являются схемы мошенничества, в которых применяются методы социальной инженерии.

Согласно данным отчета, размещенного на официальном сайте ЦБ РФ, в 2018 году с использованием методов социальной инженерии было совершено более 97% хищений со счетов физических лиц и 39% - со счетов юридических лиц. Это так называемые: телефонное мошенничество совершенные с помощью звонков или направления смс-сообщений, включая сообщения в мессенджеры.

Помимо данных видов мошенничества, не менее опасными являются мошенничества, совершенные в интернет - пространстве, с применением платежных систем и мобильного банка, при совершении

финансовых операций в банкоматах, небанковских платежных терминалах, а также другие финансовые «разводы».

Мошенничество в современных реалиях уже давно стало стилем жизни и, превратилось в бизнес для одних и горем для других.

Какие цели преследуют мошенники? Конечно же, под благовидным предлогом получить или перехватить ваши персональные данные; конфиденциальную информацию о ваших банковских данных, финансовых операциях (пароли доступа, коды активации платежных операций и т. п.) для того, чтобы добраться до ваших денег/имущества и других благ! И в этом стремлении мошенники не ограничивают себя в средствах ее достижения, а также не думают о последствиях, которые будет нести другая сторона, то есть мы.

К наиболее распространенным видам мошенничества относят:

- Телефонные мошенничества
- Интернет - мошенничества
- Интернет и мобильный банк. Платежные системы.
- При совершении финансовых операций в банкоматах, небанковских платежных терминалах
- Прочие финансовые «разводы»

Телефонные мошенничества: звонки и смс-сообщения

Каждый день, мошенники оттачивают свое мастерство и придумывают все новые и новые методы телефонного мошенничества. Тысячи людей каждый день получают звонки от злоумышленников, которые хотят украсть их деньги обманным путем.

Какие предлоги чаще всего используют мошенники при общении с жертвой?

Обычно в общении с «жертвой» используются следующие предлоги и методы:
1. Мошенники звонят с коротких номеров, представляясь сотрудником различных организации и предлагают несуществующие товары и/или услуги
2. Банковская карта заблокирована, для разблокировки звонит якобы сотрудник банка и предлагает действовать по его инструкциям.
4. Мошенники вводят вас в заблуждение манипулируя безопасностью родных, знакомых, а также играют на ваших слабостях
5. Говорит служба поддержки. Наберите на клавиатуре телефона «звездочку», а потом цифры….
6. Ошибся, указывая номер телефона, сообщите код, который пришел Вам….
7. Просьба звонка на улице.
8. Вы продаете (вещь)?... Я вам доверяю и готов оплатить ее… Мне нужно привязать Вашу карту к моему счету, продиктуйте пароль, который придет к Вам в СМС…
9. Получение дорогостоящего приза: на мобильный телефон абонента звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем (телефон, ноутбук, автомобиль) в лотерее, организованной радиостанцией и оператором мобильной связи;

ВАЖНО! Обратить внимание слушателей. ***Новый способ мошенничества.*** *Аферисты, представляясь сотрудниками кредитной организации, теперь не просят предоставить личные данные, но сообщают о попытке вывести средства со счета. И предлагают заблокировать незаконную операцию при помощи программы teamviewer. Уже поставлен рекорд незаконного списания с карты — 3,5 млн. руб.*

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Пример*: «Недавно на экране моего мобильного телефона высветился входящий городской вызов. Собеседник обратился по имени и представился сотрудником банка. Этот человек сказал, что его звонок — попытка помочь мне. Так как банку стала очевидна несанкционированная попытка перевода моих денежных средств в другом регионе». В целях безопасности счетов, «сотрудник банка» предложить сверить устройства, имеющие доступ к личному кабинету. После определения операционной системы устройства, мошенники предлагали отключить лишнюю ОС с помощью программы teamviewer*

Вот примеры телефонного мошенничества через СМС-оповещения

1. СМС с информацией о выигрыше и предложением направить ответное СМС, позвонить, отписаться от рассылки
2. СМС от якобы друга/родственника с просьбой срочно перевести деньги
3. СМС со ссылкой, по которой нужно обязательно перейти
4. СМС с информацией, что у вас задолженность по кредиту и просьбой перезвонить по указанному номеру
5. СМС с короткого номера о зачислении денег и следом с просьбой вернуть деньги
6. Необходимость решить какую-либо проблему, о чем абоненту направляется СМС-сообщение с просьбой позвонить по определенному номеру, если номер недоступен – положить на него определенную сумму и перезвонить;
7. Задержание родственника сотрудниками полиции за совершение преступления (совершение ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений и др.);
8. Все вышесказанное, но в большем объеме, мошенники распространяют в мессенджерах.

Как итог, вам пишут/звонят не друзья, а мошенники. Вы попадаете на «фишинговые» сайты, на которых передаете свои персональные данные или устанавливаете вредоносное ПО

Направляете ответное СМС или звонок оказываются платными или очень дорогими.

К сожалению, на перечисленных схемах обмана, мошенники не останавливаются. Все больший интерес мошенники проявляют к персональным данным и всеми неправдами пытаются их получить.

Финансовые мошенничества при совершении финансовых операций с применением интернет и мобильного банка, платежных систем.

Еще одним плацдармом, действия мошенников на котором становятся все масштабней и активней, является интернет и соответственно платежи, осуществляемые нами в сети.

Риски и угрозы связаны с тем, что многими Интернет воспринимается как что-то нереальное и осуществляя платежи электронными деньгами, мы соответственно не осознаем реальность операции. Когда мы рассчитываемся наличными, мы более взвешенно принимаем решение.

Федеральный закон № 161-ФЗ дает следующее определение: "Электронные деньги (ЭДС) – это безналичные денежные средства в рублях или иностранной валюте, учитываемые кредитными организациями без открытия банковского счета и переводимые с использованием электронных средств платежа".

Так в чем заключаются основные риски?

- Во-первых, Использование открытых общедоступных сетей WI-FI (транспорт, кафе, магазины) для работы в Интернет банке и мобильном банке. Такое соединение имеет слабую защиту, и соответственно, мошенники могут легко получить доступ к вашему устройству.
- Во-вторых, недостаточно высокий уровень безопасности в отдельных платежных системах (однофакторная защита).

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Двухфакторная аутентификация — это метод идентификации пользователя в каком-либо сервисе (как правило, в Интернете) при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения. На практике это обычно выглядит так: первый рубеж — это логин и пароль, второй — специальный код, приходящий по SMS или электронной почте. Реже второй «слой» защиты запрашивает специальный USB-ключ или биометрические данные пользователя. В общем, суть подхода очень проста: чтобы куда-то попасть, нужно дважды подтвердить тот факт, что вы — это вы, причем при помощи двух «ключей», одним из которых вы владеете, а другой держите в памяти.

- В-третьих, мошенниками распространяются «поддельные» программы и создаются сайты обманки, внешне очень похожие, практически неотличимые от настоящего сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные и они станут известны мошенникам. Получение мошенниками доступа **к Apple Pay и Google Pay** через NFC
- В-четвертых, электронные деньги не застрахованы государством.

Клиенты Сбербанка столкнулись с новым видом мошенничества — злоумышленники звонят с номеров самого банка, якобы предупреждая о попытке списать деньги с карты. Сбербанк внимательно изучает эти случаи и советует клиентам перезванивать, если у них возникают подозрения.

Мошенники представляются сотрудниками банка, причем располагают информацией, необходимой для подтверждения личности сотрудника. Они сообщают клиенту о блокировке попытки списать деньги с карты и под этим предлогом выведывают данные карт.

Интернет - мошенничества

Мошенничество в интернете осуществляется по схемам, известным до возникновения всемирной сети. Меняются лишь нюансы, связанные с использованием технологических достижений.

К распространенным формам обмана в сети относят следующее:

- Подделка сайта путем незначительного изменения адреса сайта и завлечение пользователей на данный сайт
- Похищение данных при их передаче оператору-злоумышленнику на поддельном сайте
- «Фальшивые» интернет-магазины – предоставление некачественного товара или не представление его совсем, завышение цен на товары, получение предоплаты за несуществующий товар.
- «Ваш аккаунт заблокирован», пришлите смс для получения кода доступа или перейдите по ссылке
- мошенничество на доверии (старый знакомый по переписке неожиданно “попадает в сложную жизненную ситуацию” и просит занять денег);
- рассылку электронных писем с уверениями, что получатель выиграл приз в лотерею;
- невыплату денег за удаленную работу;
- блокировку операционных систем или аккаунтов в социальных сетях при помощи вирусов, для удаления которых просят отправить СМС на указанный номер;
- выманивание платежных данных посредством размещения ссылок в социальных сетях и в рекламных письмах на e-mail о продаже "брендовых" товаров по низким ценам.
- и т.п.

После этих историй может сложиться обманчивое впечатление, что интернет полон угроз, и повсюду неискушенного пользователя ожидают ловушки. На самом деле доля опасных сайтов не так велика по сравнению со всеми сайтами рунета.

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Помимо социальной инженерии и интернет - мошенничества, злоумышленники воруют деньги с карт посредством банковских и небанковских платежных терминалов. Мошенники, объединённые в организованные преступные группы, действуют более масштабно и создают целые поддельные банкоматы.

Финансовые мошенничества при совершении финансовых операций с применением банкоматов, небанковских платежных терминалов

К самым распространенным способам мошенничества с применением банкоматов и небанковских платежных терминалов относят:

1. Использование «фальшивых» терминалов для осуществления платежей. Такие терминалы используют не кредитные организации, взимая, как правило, большие комиссии за осуществление платежей. В худшем случае деньги можно вообще потерять.

2. У мошенников в запасе очень много специальных приспособлений для считывания информации с карт и удерживания денежных средств в банкоматах с целью дальнейшего их изъятия. Все эти приспособления имеют даже специальное наименование:

- **Кардинг** – вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтверждённая её держателем.
- **Скотч-метод** – получение наличных путем заклеивания скотчем
- **Скимминг** – вид мошенничества с банковскими картами, который предусматривает использование различных устройств типа – скиммер. С помощью таких устройств мошенники считывают информацию, содержащуюся на магнитной полосе карты. Скиммеры, как правило, прикрепляются к банкоматам, а именно – к принимающему слоту.
- **Шимминг-** является одним из наиболее опасных способов мошенничества с банковским «пластиком», который является усовершенствованной разновидностью известного всем скимминга. Благодаря этой технологии при помощи банкомата злоумышленник может легко узнать номер и PIN-код карты своей жертвы.
- **Трапинг-** Использование специальных приспособлений для блокировки пластиковой карты в банкоматах (трапинг).
- **«Ливанская петля»** Ловля карты в приемнике карты (с помощью ленты)

3. Новый способ мошенничества с банкоматом - здесь используется рабочий сценарий банковских терминалов. В частности, злоумышленник начинает операцию, не требующую карты, например, пытается перевести средства на нужный ему номер телефона. В завершающий момент операции на экране устройства возникает требование ввести карту и пин-код.

После этого злоумышленник отходит от терминала. Подошедший за ним клиент банка видит на дисплее устройства картину, напоминающую стартовый экран работы с предложением ввести карту. Он выполняет то, что требует машина, поскольку полагает, что это необходимо для начала работы с терминалом. Затем с его карты немедленно списываются средства по операции предыдущего «клиента».

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Правила финансовой гигиены для защиты от мошенников

Предлагаю следовать следующим правилам безопасности:

1. Телефонные мошенничества (звонки и смс-сообщения):

- Во-первых, – не волноваться и не поддаваться панике, связаться с "пострадавшими" родственниками и обратиться в полицию! Ни в коем случае не передавать деньги незнакомым людям!
- Во-вторых, не торопиться сообщать реквизиты вашей карты! Никто, включая банк, не вправе требовать данные вашей пластиковой карты! Для того, чтобы проверить поступившую информацию о блокировании карты, необходимо позвонить в клиентскую службу поддержки банка.
- В-третьих, оформление крупного выигрыша никогда не происходит только по телефону или Интернету.
- В-четвертых, для возврата средств при якобы ошибочном переводе существует чек. Не возвращайте деньги сразу, не разобравшись в ситуации.

2. Финансовые мошенничества при совершении финансовых операций с применением интернет и мобильного банка, платежных систем.

- Подключите СМС-уведомления по банковской карте и электронному кошельку и отслеживайте движение и остаток средств.
- Сообщайте в финансовую организацию, если кошелек «взломан», карта потерялась, данные карты стали известны посторонним или с нее без согласия держателя списаны деньги.
- Не допускайте посторонних к банковской карте, электронному кошельку, мобильному телефону и компьютеру.
- Используйте сложные и разные пароли, не сохраняйте их в интернет-сервисах.
- Старайтесь не открывать сайты платежных систем по ссылке (например, в письмах). Обязательно проверяйте, какой URL стоит в адресной строке, или посмотрите в свойствах ссылки, куда она ведет.

3. Интернет-мошенничество

Просто, как и в реальной жизни, при работе в сети интернет не стоит терять бдительность. А соблюдение простых правил позволит вам избежать большинства проблем:

- Задайте надежный пароль для точки доступа. Аналогичным образом поступите с паролем для беспроводной сети. Чем сложнее — тем лучше. Не используйте простые варианты.
- Скройте имя сети: после настройки всех домашних устройств на работу с Wi-Fi скройте имя сети (SSID).
- Отключите WPS: эта функция позволяет быстро добавить устройство к сети с помощью ПИН-кода.
- С публичными сетями сложнее. Даже их владелец, имеющий доступ к настройкам роутера, не может гарантировать безопасность. Поэтому не работайте с критически важными данными, выходя в Интернет с помощью публичных сетей.
- Выключите автоматическое подключение к Wi-Fi. Таким образом вы убережете свой смартфон или ноутбук от подключения к фальшивой точке доступа.
- Используйте VPN. Если вам приходится часто работать в разъездах и при этом использовать публичный Wi-Fi, VPN — самый надежный способ обезопасить себя. Однако необходимо помнить, что это платная услуга.
- Работайте с защищенными приложениями.
- Никогда и никому не сообщайте ваши пароли. Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях.

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

БОГАТЕЙ С ДЕТСТВА

- Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку. Настоящие работодатели никогда не просят денег с соискателей, они сами платят за работу!
- Предложения в духе «вышлите туда-то небольшую сумму и вскоре вы будете завалены деньгами» — это предложения от участников финансовых пирамид. Не верьте таким предложениям, в пирамидах выигрывают только их создатели.
- Письма о проблемах с вашим счетом в какой-либо платежной системе, требующие перехода на сайт и каких-либо действий от вас, отправляйте в корзину, не открывая. Техническая поддержка платежных систем никогда не рассылает таких писем.
- В 99 % случаев платежи, которые вы делаете онлайн, отменить нельзя. Поэтому не торопитесь, подумайте, прежде чем заплатить за товар или услугу.

4. Банкоматы, небанковские платежные терминалы.

- Подключите СМС-информирование в целях безопасности и контроля за вашими денежными средствами.
- Не сообщайте никому CVV-код и одноразовый пароль.
- При пользовании банкоматом проявляйте осторожность, обращайте внимание на посторонних вокруг и подозрительные устройства, и накладки в местах ввода ПИН-кода и карты.
- Заранее узнайте, какова комиссия по вашему платежу.

Мошенники не стоят на месте, постоянно совершенствуясь, соответственно и расширяется список используемых ими инструментов, характерным отличием которых от иных способов является маскирование под «традиционные» виды деятельности, например, юристы-аферисты, раздолжнители, лжебанки и т.п.

Новые виды мошенничества и прочие «разводы»

1. В сети интернет очень много предложений юристов, способных решить любые проблемы с банками по задолженности по кредитам. С экранов телевизоров нам "жертвы банков" рассказывают о том, как квалифицированно, быстро и бесплатно им помогли. Что происходит на самом деле? Юридические компании зарабатывают на обещаниях и гарантируют то, что выполнить невозможно, взимая плату за оказанные "консультационные" услуги и не решая при этом никаких проблем.
2. Появляются "лжебанки", предлагающие людям с испорченной кредитной историей оформить кредиты по ставкам ниже банковских. Правда чтобы якобы получить деньги, надо внести первоначальный взнос в размере 5-20% от требуемой суммы.
3. Мало того банки, стали продавать продукт, маскируя его под банковский продукт. Например, предложение страховых полисов под видом депозита. Страховые вклады Агентством по страхованию вкладов НЕ застрахованы! В случае банкротства организации, никто ничего не возместит. Доходность не гарантирована.

Глоссарий

Антиколлекторы — они же **«раздолжнители», кредитные юристы** — это компании или частные лица, которые предлагают решить проблемы с просроченным долгом или зарабатывающие на обещаниях и гарантирующие то, что невозможно.

Банковская карта - пластиковая карточка, дающая своему владельцу доступ к его счету в банке и позволяющая осуществлять различные операции, в том числе оплату покупок и получение наличных денег.

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

Банкомат — это автоматическое устройство для выдачи наличных денег по банковской пластиковой карточке и проведения других операций с банковским счётом.

Бинарные опционы - упрощенный вариант Форекс. Опцион – это ставка на событие (рост или падение цены). Угадал – получил выигрыш, нет – потерял ставку. При этом активы не приобретаются. Высокорисковый инвестиционный инструмент, высока вероятность потерять вложенные деньги.

Валютный (девальвации) риск — вероятность снижения стоимости валюты, в которую были вложены средства. Для того чтобы бороться с риском девальвации, необходимо хранить сбережения **в нескольких разных валютах**, можно разместить свои сбережения на депозиты в разных валютах.

Инвестиционный риск — вероятность финансовых потерь в процессе инвестиционной деятельности.

Интернет-магазин (англ. online shop или e-shop) — сайт, торгующий товарами посредством сети Интернет.

Инфляционный риск — вероятность снижения стоимости сбережений и инвестиций из-за инфляции.

Кардинг – это использование украденных банковских карт или их платёжных реквизитов.

Магазинные мошенничества – вид мошенничества, когда во время оплаты покупки или услуги данные карты могут быть считаны и зафиксированы ручным скиммером.

Мошенничество – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Мобильный банк, Интернет-банк - технология предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом, чаще всего с использованием компьютерных и телефонных сетей.

Платежная система- это сервис для перевода денег или иных средств, их заменяющих (чеки, сертификаты, условные платёжные единицы или специализированные ценные бумаги), в электронной или физической форме (далее денежные средства). Платежная система устанавливает определенный набор правил, программных, аппаратных и технических средств для передачи денежных средств от одной стороны другой.

Платёжный терминал (self-service terminals, SSTs) — аппаратно-программный комплекс, обеспечивающий приём платежей от физических лиц в режиме самообслуживания.

Рыночный (ценовой) риск — вероятность изменения рыночной цены объекта инвестиций (акций, облигаций, золота и т. п.).

Риск мошенничества — вероятность потери вложенных средств из-за неправомерных действий, обмана

Смишинг – это мошенническая операция, проводимая с помощью СМС-сообщений.

Скиммер – инструмент злоумышленника для считывания, например, магнитной дорожки платёжной карты.

Скимминг – мошенническая схема в основе которой лежит использование специального считывающего устройство (скиммера), устанавливаемого на банкомат.

Траппинг - установке на банкомат устройства, которое блокирует карту и не выдает ее обратно, а «добрый» прохожий, якобы пытающийся помочь, подглядывает пин-код и после вашего ухода, забирает карту из банкомата и снимает с нее деньги.

Трейдер - сотрудник брокерской фирмы, выполняющий заказы клиентов на куплю-продажу ценных бумаг на бирже.

Фишинг – это создание мошенниками ложного сайта с целью принуждения владельца банковской карты предоставить злоумышленникам свои конфиденциальные данные, платёжные реквизиты, регистрационное имя, пароль или секретный пин-код.

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

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ
ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ

БОГАТЕЙ С ДЕТСТВА

Финансовая пирамида – схема инвестиционного мошенничества, в которой доход по привлеченным денежным средствам образуется не за счет вложения их в прибыльные активы, а за счет поступления денежных средств от привлечения новых инвесторов. человеку обязательно знать признаки подобных схем, уметь их распознавать и избегать.

Финансовая подушка безопасности (резервный фонд) - запас денежных средств и других ценностей на случай лишения доходов по причине непредвиденных обстоятельств, таких как потеря работы, болезнь, несчастный случай.

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

Forex (от англ. FOReign EXchange - «зарубежный обмен») - рынок обмена валюты по свободным ценам, который формирует непрерывный процесс обмена одной иностранной валюты на другую. Высокорисковый инвестиционный инструмент, высока вероятность потерять вложенные деньги.

ПРОЕКТ РЕАЛИЗУЕТСЯ ПРИ ПОДДЕРЖКЕ
ФОНДА ПРЕЗИДЕНТСКИХ ГРАНТОВ