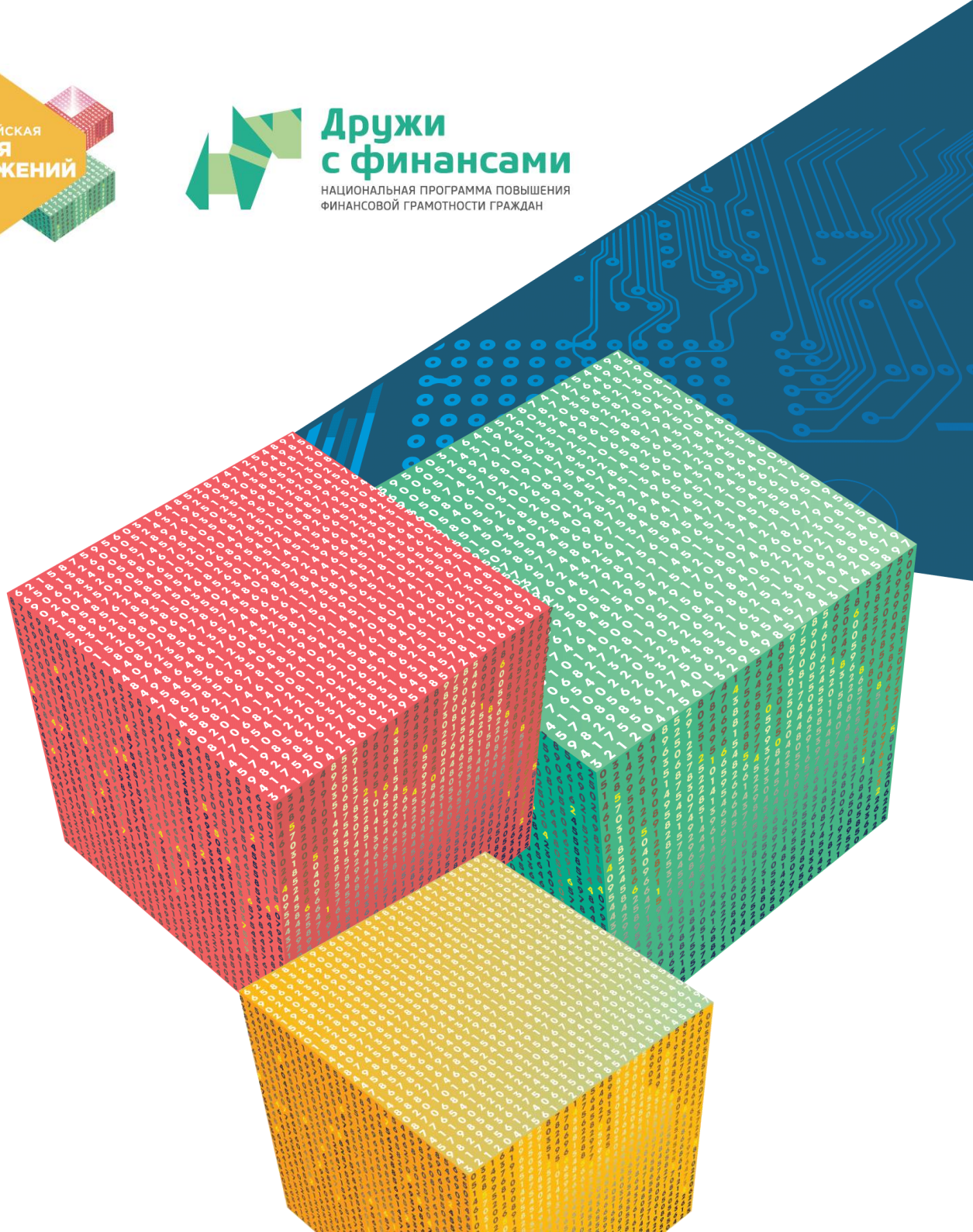
МИНИСТЕРСТВО ФИНАНСОВ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ВСЕРОССИЙСКАЯ
НЕДЕЛЯ
СБЕРЕЖЕНИЙ

Дружи
с финансами
НАЦИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ
ФИНАНСОВОЙ ГРАМОТНОСТИ ГРАЖДАН

Основы финансовой безопасности



вашифинансы.рф

ФИО спикера

Самопрезентация – кто, компания, общая информация

Достижения:

- Информация о спикере заполняется самим спикером в рамках подготовки к презентации

Фото / логотип/ ...

Финансовая грамотность

Вопросы финансов затрагивают все сферы жизни современного человека, а финансовая грамотность стала необходимым жизненным навыком, как умение читать и писать. Финансово грамотный человек подсчитывает свои расходы и доходы, ведёт семейный или личный бюджет, не влезает в излишние долги, имеет финансовую «подушку безопасности». Финансовая грамотность дает возможность управлять своим финансовым благополучием, строить долгосрочные планы и добиваться успеха.

Проект «Содействие повышению уровня финансовой грамотности населения и развитию финансового образования в Российской Федерации» реализуется Министерством финансов Российской Федерации совместно с Всемирным банком.

Цель - повышение финансовой грамотности российских граждан, содействие формированию у населения разумного финансового поведения, обоснованных решений, ответственного отношения к личным финансам.

Финансовая безопасность – это про что?

- Пережить временные финансовые трудности (или смягчить их последствия) не снижая уровень жизни и не залезая в долги
- Избежать вложений денег в финансовые пирамиды или высокорискованные инструменты (тем более, взяв на это кредит)
- «Охранять» деньги от мошенников при совершении переводов, платежей и покупки услуг, в том числе, с использованием цифровых сервисов

Программа «Цифровая экономика Российской Федерации»: утв. распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р

Цифровая экономика – это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг

Цифровизация – замена физических систем сбора и обработки данных технологическими системами, которые генерируют, передают и обрабатывают цифровой сигнал о своем состоянии

Цифровая среда современного человека:

- диджитализация – настоящий бум жизни онлайн;
- мультиэкранность – Smart-TV, компьютеры, планшеты, смартфоны

Элементы цифровизации

Диджитализация – перевод содержания бизнес-процессов в цифровой формат

Облачные технологии – электронное хранилище данных в сети Интернет

Интернет вещей – сеть физических объектов со встроенной электроникой, способной общаться с другими объектами
Например: «умный дом», чайник, управляемый со смартфона и т.д.

Искусственный интеллект – свойство интеллектуальных систем выполнять творческие функции

Большие данные (Big Data) – агрегированные данные, предварительно подготовленные для их эффективной обработки

Виртуальная реальность – созданный техническими средствами мир, передаваемый человеку через его ощущения

Дополненная реальность - результат введения в поле зрения сенсорных данных с целью дополнения сведений об окружении и улучшения

«Плюсы» цифровой экономики для потребителей финансовых услуг

- Упрощение финансовых операций, повышение роли электронных и цифровых денег
- Упрощение платежей
- Сокращение затрат
- Удобство доступа
- Гибкость продуктов
- Быстрое информирование клиента
- Возможность получить отчет и проанализировать операции
- Развитие возможностей дистанционной работы
- Внедрение электронного документооборота
- Более открытый и доступный финансовый рынок
- Повышение финансовой грамотности

Цифровые сервисы и инструменты в сфере финансов для населения

- Сервисы по проведению платежей и оплате покупок
- Сервисы по кредитованию и частным займам, по страхованию, анализу финансовой истории
- Сервисы по управлению личными финансами, по финансовому планированию
- Продукты для повышения финансовой грамотности
- Новые технологии и инструменты финансовых операций

Способы управления движением безналичных денег

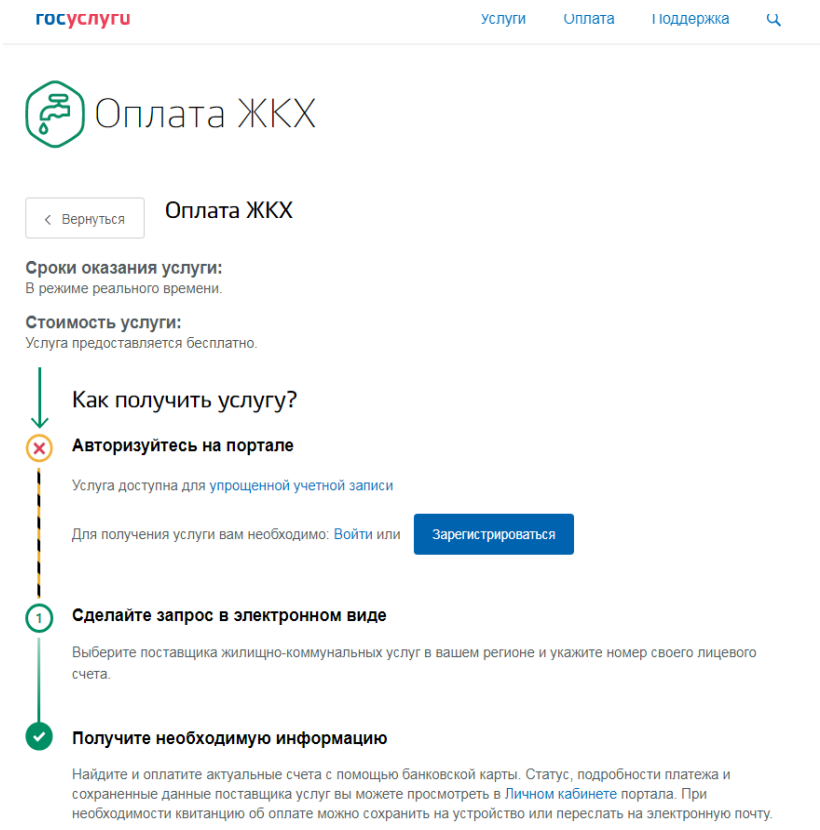
- отделение соответствующей организации (банка, системы денежных переводов, почты, салона связи и других
- платежный терминал банка
- карта – банковская карта, карта к электронному кошельку, платежная карта
- Интернет-банкинг для управления банковской картой
- Система Быстрых Платежей (новый сервис Банка России – СБП)
- электронный кошелек

Онлайн-платежи по оплате услуг ЖКХ, налогов, госпошлины, штрафов ГИБДД:

– зарегистрируйтесь на официальном портале www.nalog.ru и/или www.gosuslugi.ru;

– вы можете подавать заявку на получение ряда услуг, получать уведомления, заполнять необходимые документы и оплачивать налоги, штрафы, услуги;

– можно воспользоваться возможностью получить скидку на оплату госпошлины, штрафов



Риски цифровой экономики для потребителей финансовых услуг

- риск киберугроз, связанный с проблемой защиты персональных данных;

-«цифровое рабство» – использование данных о человеке для управления его поведением;

-«цифровой разрыв» – разрыв в цифровом образовании, в условиях доступа к цифровым услугам и продуктам, и, как следствие, разрыв в уровне благосостояния людей;

- недостаточная прозрачность цен и условий;

- сложность подачи жалоб;

- риски нерационального поведения на финансовом рынке как следствие доступности операций для неквалифицированных потребителей финансовых услуг;

- риски подверженности новым инструментам мошенничества с использованием цифровых технологий

Что делать?

Повышать уровень финансовой грамотности!

Риски в пользовании цифровыми финансовыми услугами*

34% – Рисков нет

15% – Риски примерно одинаковые с традиционными видами услуг

33% – Риски есть: мошенники / хакеры / воровство / взлом карты / личного кабинета

18% – Затрудняюсь ответить

* – по данным НАФИ

Финансовая безопасность

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

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

- Мошенничества с использованием банковских карт
- Интернет-мошенничества
- Мобильные мошенничества
- Финансовые пирамиды
- Кредит в продаже медицинских услуг

ВСЕРОССИЙСКАЯ НЕДЕЛЯ СБЕРЕЖЕНИЙ

Мошенничества с использованиям банковских карт

вашифинансы.рф

КАРТА

7 из 10 совершеннолетних россиян владеют банковскими картами*

Банковская карта – удобный инструмент повседневных расчетов.

Наиболее распространены:

- Дебетовые - инструмент управления банковским счетом, на котором размещены собственные средства держателя карты.
- Кредитные - это банковская пластиковая карта, позволяющая на основании заключенного с банком договора брать в долг у банка определенные суммы денег в пределах установленного кредитного лимита.

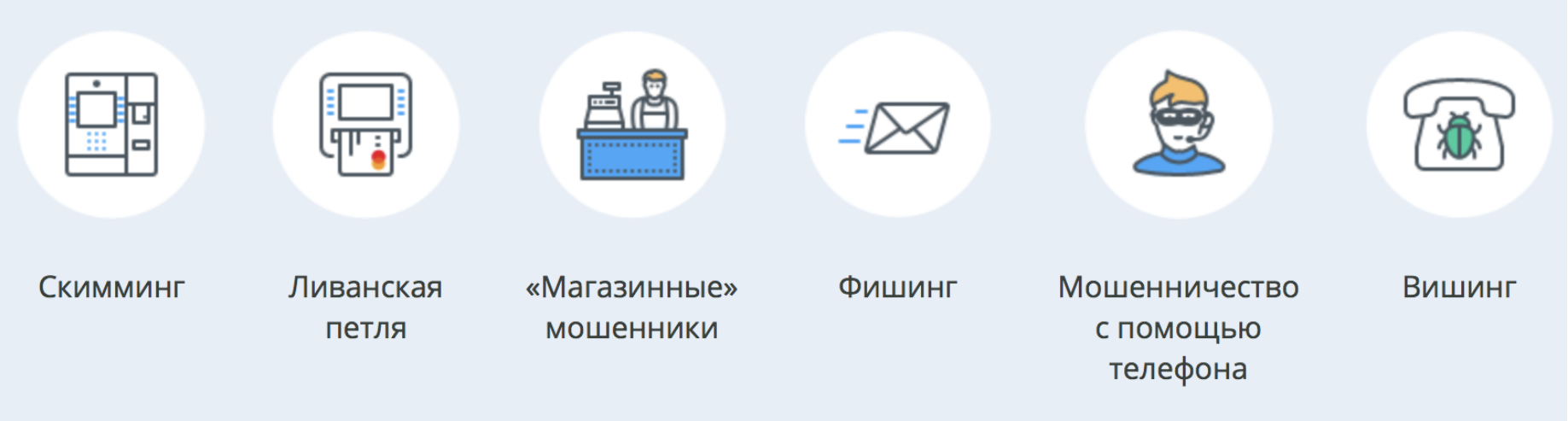
Способы финансового мошенничества с банковскими картами

- Мошенники не знают реквизиты банковской карты: владелец карты сам совершает действия по переводу средств со своей карты на счет мошенников

- Мошенники получают обманным путем реквизиты банковской карты: кража с карты осуществляется с помощью технических средств (скимминг), фишинга, претекстинга (социальной инженерии)

- Мошенники крадут данные / карту без участия владельца: кража данных – с серверов реальных интернет-магазинов, через недобросовестных сотрудников банка, кража пластиковой карты

Схемы мошенничеств с картами



Способы обмана людей и кражи денег с их банковских карт разнообразны: от подглядывания из-за плеча во время операций с банкоматом и последующего хищения карты до хакерских атак на программное обеспечение. При этом преступники постоянно придумывают новые способы хищения денежных средств, по мере того как старые перестают работать. Именно поэтому важно быть в курсе основных приемов, которые используют злоумышленники, и соблюдать базовые правила безопасности.

Скимминг

Предполагает установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте.

Таковыми выступают накладная клавиатура (очень похожая на настоящую) и устройство для считывания данных карты, которое устанавливается на картридер

Вместо клавиатуры может быть установлена миниатюрная камера, которая заснимет процесс **ввода ПИН-кода**.

При использовании банкомата осмотрите поверхность над ПИН-клавиатурой и устройство для приема карты на предмет нахождения посторонних предметов.

Траппинг (ливанская петля)

или помощь прохожего. Суть этого вида мошенничества заключается в установке на банкомат устройства, которое **блокирует карту и не выдает ее обратно**.

Отрезок фотопленки (складывается пополам, края загибаются под углом в 90 градусов) вставляется в банкомат. На нижней стороне фотопленки вырезан небольшой лепесток, отогнутый вверх по ходу карты. Пленка располагается в картридере так, чтобы не мешать проведению транзакции. Отогнувшийся лепесток не позволяет банкомату выдать пластиковую карту обратно.

На помощь человеку приходит «добрый» мошенник, раздавая различные советы. В процессе «помощи» растерянный человек обычно соглашается на введение ПИН-кода, который и запоминает преступник. После чего мошенник «уходит», советуя обратиться в банк. Растерянный человек оставляет карту в банкомате, а мошенник спокойно ее достает и использует по своему усмотрению.

Закрывайте рукой клавиатуру при вводе ПИН-кода

Магазинные мошенничества

От недобросовестных сотрудников в организациях не застрахован никто. Данные карты могут быть считаны и зафиксированы ручным скиммером, а впоследствии использованы для хищения денег.

- Не передавайте карту посторонним: ее реквизиты (номер карты, срок действия, имя владельца, CVV/CVC-код) могут быть использованы для чужих покупок
- Требуйте проведения операций с картой только в личном присутствии, не позволяя уносить карту из поля зрения (например, официантам или кассирам)

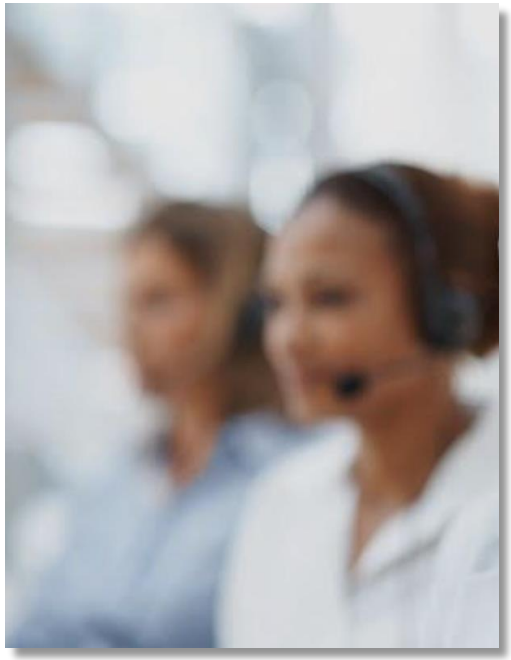
Фишинг

Цель фишинга — получить данные о пластиковой карте от самого пользователя. В этом случае злоумышленники рассылают пользователям электронные письма, в которых от имени банка сообщают об изменениях, якобы производимых в системе его безопасности.

При этом мошенники просят доверчивых пользователей возобновить информацию о карте, в том числе указать номер кредитки и ее ПИН-код. Сделать это предлагается несколькими способами: либо отправив ответное письмо, либо пройдя на сайт банка-эмитента и заполнив соответствующую анкету. Однако ссылка, прикрепленная к письму, ведет не на ресурс банка, а на поддельный сайт, имитирующий работу настоящего.

Самая сложная задача мошенника — узнать ваш ПИН-код. Никому не сообщайте свой ПИН-код.

Мошенничество с помощью телефона



Разновидностью фишинга являются звонки на сотовые телефоны граждан от «представителей» банка с просьбой погасить задолженность по кредиту.

Когда гражданин сообщает, что кредит он не брал, ему предлагается уточнить данные его пластиковой карты.

В дальнейшем указанная информация используется для инициирования несанкционированных денежных переводов с карточного счета пользователя.

Банки и платежные системы никогда не присылают писем и не звонят на телефоны своих клиентов с просьбой предоставить им данные счетов. Если такая ситуация произойдет, вас попросят приехать в банк лично.

Вишинг (голосовой фишинг)

Новый вид мошенничества, использующий технологию, позволяющую автоматически собирать информацию, такую, как номера карт и счетов.

Мошенники моделируют звонок автоинформатора, получив который держатель получает следующую информацию:

- Автоответчик предупреждает потребителя, что с его картой производятся мошеннические действия, и дает инструкции — перезвонить по определенному номеру. Злоумышленник, принимающий звонки по указанному автоответчиком номеру, представляется вымышленным именем от лица финансовой организации.
- Когда по этому номеру перезванивают, на другом конце провода отвечает типичный компьютерный голос, сообщающий, что человек должен пройти сверку данных и ввести 16-значный номер карты с клавиатуры телефона.
- Затем, используя этот звонок, можно собрать и дополнительную информацию, такую, как CVV-код, срок действия карты, дата рождения, номер банковского счета и т. п.

Меры безопасности

Несмотря на все системы информационной безопасности банка в результате мошеннических операций с картами существует отличная от нуля вероятность хищения средств с вашей карты. Чтобы избежать исчезновения денег, соблюдайте правила, затрудняющие неправомерные операции с вашими финансами:

- Храните ПИН-код отдельно от карты и не пишите его на карте, не сообщайте никому и не вводите ПИН-код при работе в Интернете. При его потере или краже -заблокируйте карту
- Сохраняйте все документы до окончания проверки правильности списанных сумм
- Сообщайте банку актуальные контактные данные
- Подключите услугу SMS- уведомлений, всегда имейте при себе телефон службы поддержки

Структура мошенничества с банковскими картами в России. Всего 4,48 млрд. руб.

В случае мошеннической или ошибочной операции по карте уведомите банк до конца следующего дня, чтобы сумма этой операции была полностью возмещена банком, иначе вернуть деньги будет гораздо сложнее.

При расчете картами

- Не превышайте лимит кредитования – это может приводить к блокированию карты, штрафам и комиссиям
- Своевременно оплачивайте кредит – это обеспечит отличную кредитную историю и убережет от штрафов
- Не допускайте потери карты, поломки, блокировки - перевыпуск карты может стоить дополнительных средств
- Не снимайте с карты деньги полностью – оставьте сумму для оплаты комиссий или автоматических платежей. В случае отсутствия суммы и если карта предусматривает овердрафт, банк совершит данный платеж за счет заемных средств.
- Если сменили место работы уточните актуальные для вас тарифы по зарплатной карте
- При использовании карты зарубежом, помните о курсовой разнице. Если карта привязана к рублевому счету, то при расчетах за границей банкоматы и платежные терминалы будут использовать один курс, а российский банк спишет деньги со счета, применяя другой, и может возникнуть нежелательный «технический овердрафт».

Социальная инженерия – как нами манипулируют

Приемы социальной инженерии

1. Предъявляется «приманка», формирующая положительные (выигрыш в лотерею, оплата выставленного вами на продажу товара), или негативные эмоции (претензия по неоплаченному налогу, взыскание по долгу коллекторским агентством, несанкционированное списание средств со счета, блокировка карты).
2. Злоумышленник представляется сотрудником государственных органов, банка, страховой компании, электронного магазина и т.д
3. Создается дефицит времени для принятия решения: «чтобы приз не ушел к другому, перезвонить или сообщить свои данные нужно в ближайшие пять минут», «чтобы избежать повестки суд, необходимо оплатить задолженность в течение 24 часов» и т.д.

Результат

В условиях необходимости быстрого реагирования наш мозг автоматически переводится в режим стресса. Мы следуем инструкциям мошенников

Социальная инженерия – что делать в ответ

Во-первых, необходимо осознать, что тебя ставят в условия немедленного принятия решения, и зажечь «красную лампочку». Покупки-продажи финансовых продуктов и услуг не должны совершаться в течение ближайших 5 минут.

Во-вторых, необходимо любыми способами убрать влияние дефицита времени, взять паузу. Если собеседник говорит вам «Сейчас или никогда!», смотри пункт первый.

В-третьих, успокоиться и трезво оценить ситуацию:

• медленно подышать – это один из способов снизить частоту пульса и перевести свой организм и мозг из режима быстрого реагирования в спокойный режим;

• проверить информацию, которую вы успели получить от звонившего (посмотреть в сети Интернет информацию об аналогичных ситуациях или позвонить по официальному номеру в компанию от имени которой вас ожидают призы или угрозы;

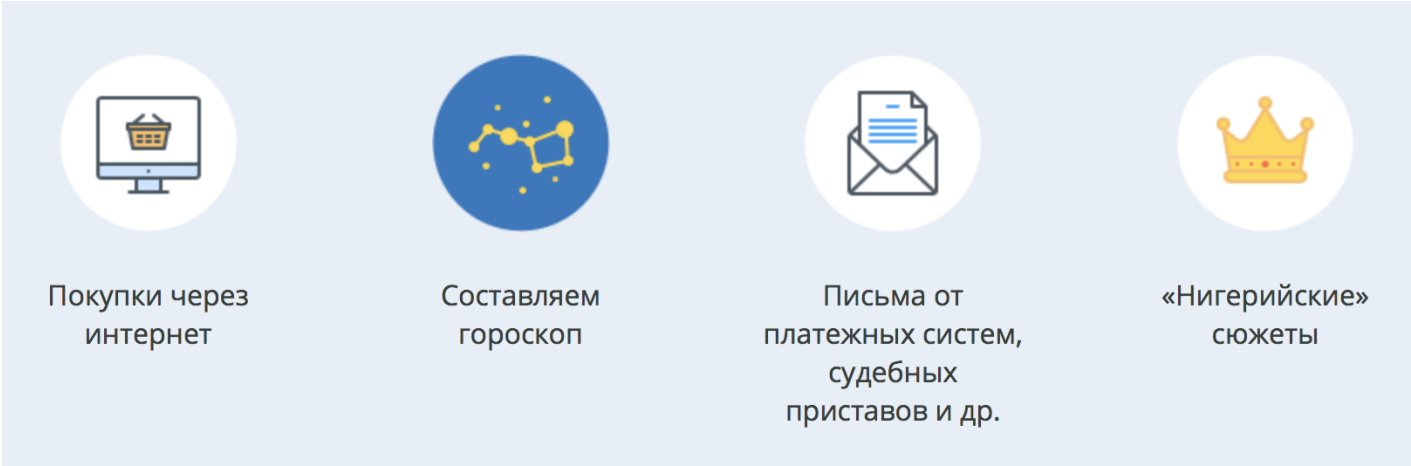
• позвонить родным, другу, кому-то, кто мог бы посмотреть на ситуацию взглядом, не замутненным эмоциями, и указать вам на риск мошенничества.

ВСЕРОССИЙСКАЯ НЕДЕЛЯ СБЕРЕЖЕНИЙ

Интернет-мошенничества

вашифинансы.рф

Виды интернет-мошенничеств



Мошенничество в интернете включает в себя все существующие виды обмана, придуманные человечеством за всю историю его существования. Этот перечень обширен, поскольку мошенники по максимуму используют все преимущества интернет-коммуникаций: массовый охват, возможность выбора целевой группы, оперативность.

Покупки через интернет

Покупатель (жертва) соглашается купить у продавца (мошенника) товар через интернет. Продавец просит оплатить товар через систему денежных переводов и получает деньги, используя зачастую фальшивое или недействительное удостоверение личности. Обещанный товар не доставляется покупателю.

Такая схема мошенничества обычно имеет один или несколько явных признаков — например, предлагаемый товар продается по **удивительно низкой цене**.

Составление гороскопа

Объявлений, предлагающих заказать персональный гороскоп, очень много во всемирной паутине. Авторы обещают выслать его быстро и бесплатно. Пользователю предлагается заполнить стандартную анкету (имя, фамилия, дата рождения), оставить свой электронный адрес.

Любитель астрологии указывает все эти данные, но вместо гороскопа в его ящик попадает письмо с еще одним условием: чтобы получить заказ, надо отправить по указанному номеру СМС-сообщение с набором тех или иных цифр. При этом забывают добавить, что стоимость этого сообщения может составлять **несколько сотен рублей**. В лучшем случае ему, действительно, пришлют гороскоп. Причем сразу же, что уже вызывает сомнения в его уникальности. В худшем — ничего не пришлют.

Письма платежных систем

Вы можете обнаружить в своем почтовом ящике письмо от администрации платежной системы (e-gold, Moneybookers, Paypal), судебных приставов и других… В послании, например, говорится, что у вас есть долг по кредиту и вам нужно срочно сверить данные в файле. К письму прилагается вложение — файл, который нужно скачать и открыть. Или же в письме есть ссылка, по которой нужно перейти «для скачивания программы».

На самом деле часто вас поджидает **вирус**, задача которого - собрать данные о ваших аккаунтах в платежных системах, **данные банковской карты**, которые вы вводите на своем компьютере.

«Нигерийские» сюжеты

Суть этой мошеннической схемы сводится к тому, что некто представляется получателю письма действующим или бывшим министром или представителем знатной нигерийской (зимбабвийской, кенийской...) семьи, попавшей в немилость на родине. К адресату обращаются с просьбой оказать содействие в выводе из охваченной гражданской войной страны крупной суммы, которая будет переведена на счет адресата. Ему за помощь «в спасении средств» обещают солидный процент. Когда клиент «заглатывает наживку», его просят перечислить незначительную сумму, необходимую для оформления перевода, дачи взятки или оплаты услуг юриста. Затем появляется еще одна причина перечислить «незначительную» сумму, потом другая... Деньги тянут из доверчивого клиента до тех пор, пока он не осознает, что его обманули.

По результатам специальных исследований, примерно один процент пользователей интернета, то есть **каждый сотый**, получивших по e-mail «нигерийские письма», оказываются вовлеченными в эту аферу. В арсенале мошенников как правило всего несколько уловок, которые могут сочетаться в одном письме.

Способы защиты

- 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. Вы можете попасть на сайт-обманку, внешне очень похожий, практически неотличимый от настоящего сайта платежной системы. Расчет в этом случае на то, что вы введете на таком сайте свои данные и они станут известны мошенникам.
- Совершайте покупки в интернете с помощью отдельной банковской карты и только на проверенных сайтах
- Никогда никому не сообщайте ваши пароли. Вводить пароли можно и нужно только на самих сайтах платежных процессоров, но никак не на других ресурсах.
- Не храните файлы с секретной информацией на доступных или недостаточно надежных носителях информации. Всегда делайте несколько копий таких файлов на разных носителях.

Способы защиты

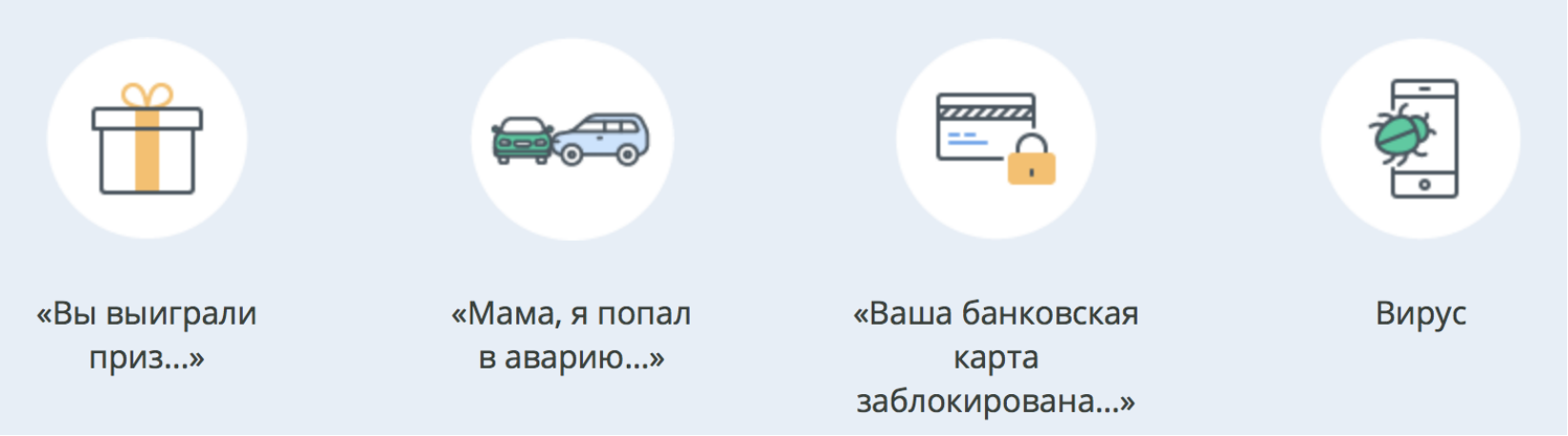
- Если вам предлагают удаленную работу и при этом просят оплатить регистрационный взнос в качестве гарантии за пересылку данных и т. п., не попадайтесь на эту ловушку. Настоящие работодатели никогда не просят денег с соискателей, они сами платят за работу!
- Предложения в духе «вышлите туда-то небольшую 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.

ВСЕРОССИЙСКАЯ НЕДЕЛЯ СБЕРЕЖЕНИЙ

Мобильные мошенничества

вашифинансы.рф

Виды мобильных мошенничеств



Основных видов мобильного мошенничества немного, но их вариаций достаточно много, причем все они выгодны для мошенников и приносят им огромные суммы денег. Даже при небольших финансовых потерях конкретного человека (15-150 рублей) срабатывает эффект масштаба, когда жертвами становятся тысячи людей.

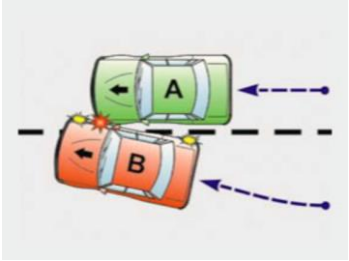
По данным международной статистики, совокупные потери операторов связи и абонентов от мобильного мошенничества ежегодно составляют **примерно 25 млрд долларов**.

«Вы выиграли приз...»

Мошенник привлекает «жертву» дорогим подарком, который выиграл абонент, но при этом просит прислать подтверждающую СМС, внести «регистрационный взнос» через интернет-кошелек, купить карточку предоплаты и перезвонить, назвав код.

Получив «взнос», мошенник исчезает, а обещанный приз тоже растворяется.

«Мама, я попал в аварию...»



Эта схема направлена на воздействие на психику человека. Мошенник отправляет СМС или звонит с неприятной новостью, «жертва» в панике забывает проверить достоверность полученной информации и переводит средства на счета мошенников.

«Ваша карта заблокирована»

На мобильный телефон приходит СМС «Ваша банковская карта заблокирована. По вопросам разблокировки обращайтесь по телефону…». «Жертва» перезванивает по указанному номеру и «сотрудник банка», которым является мошенник, предлагает пройти к банкомату и совершить несколько операций под диктовку. Результат не заставит себя долго ждать - деньги с карты перейдут на счет мошенников.

Вирус

Он помогает злоумышленникам подобраться к банковской карте, привязанной к мобильному телефону, и перевести все деньги на свой счет.

В 2014 г. сотрудники компании Tele2 приняли от абонентов и обработали 17 640 обращений с жалобами на разные виды мошенничества. На диаграмме представлены основные виды мошеннических схем.

Способы защиты

- Не отвечайте на СМС и не открывайте ММС от неизвестных абонентов, в том числе поздравительные сообщения и открытки. С вашего счета могут списать деньги.
- При получении сообщений от банков, мобильных операторов о проблемах со счетом перезвоните по известному вам номеру банка и уточните информацию. Банк никогда не сообщает подобным образом информацию.
- Не отправляете СМС на короткие номера, заранее не узнав стоимости подобного сообщения. Это можно сделать на сайте своего оператора мобильной связи.

Способы защиты

- Никогда не сообщайте никаких персональных данных (дату рождения, ФИО, данные о родственниках и т. д.), даже если вам звонят и представляются сотрудником банка, полиции, мобильных операторов и т. д. Попросите представиться, назвать ФИО, звание-должность, поинтересуйтесь, какой адрес у отделения, офиса, уточните наименование организации. Затем узнайте телефон этой организации в справочных базах и перезвоните. Помните: мошенники могут использовать ваши персональные данные в разнообразных преступных схемах, вплоть до открытия на ваше имя фирмы.
- Вам могут позвонить и сообщить, что ваш родственник или знакомый попал в аварию, за решетку, в больницу и за него нужно внести залог, штраф, взятку — откупиться. Не верьте! Позвоните вашему родственнику.
- Ценную информацию никогда не храните только в телефоне, дублируйте ее в бумажном блокноте или в компьютере.

ВСЕРОССИЙСКАЯ НЕДЕЛЯ СБЕРЕЖЕНИЙ

Как не стать жертвой финансовой Пирамиды

вашифинансы.рф

Финансовая пирамида

Если говорить о деньгах, то нами движут два основных чувства: страх потерять заработанное и желание максимально преумножить то, что уже есть. К сожалению, часто именно второе чувство притупляет осторожность и приводит к плачевным финансовым результатам.

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.

Принцип работы

Инвесторов побуждают вкладывать денежные средства обещанием получения высокой гарантированной доходности. Поскольку нет возможности обеспечить в течение длительного времени постоянный приток денежных средств новых инвесторов, ресурсы финансовой пирамиды начинают сокращаться, а финансовые обязательства растут. Возможность возврата вложенных средств с течением времени становится всё меньше.

Закономерным итогом такой ситуации становится крах финансовой пирамиды, в результате которого инвесторы теряют вложенные средства.

Чтобы не стать жертвой пирамиды

Во-первых, не поддавайтесь на агрессивную рекламу «легких и быстрых денег», гарантированная доходность выше ставки банковского депозита – повод задуматься о целесообразности таких вложений.

Во-вторых, обратите внимание на следующие признаки, которые могут характеризовать организацию как «финансовую пирамиду»:

- Вам объясняют высокую доходность непрозрачными сверхприбыльными проектами, при этом не раскрывают информацию о потенциальных рисках. Проекты, как правило, находятся в другой стране, что затрудняет выяснение текущего положения дел.
- Организаторы скрывают информацию о себе, о наличии лицензий на ведение соответствующей деятельности и действуют через посредников. Часто компания зарегистрирована не в России.
- Вам обещают высокое вознаграждения за приведенных друзей, знакомых или родственников. Предлагают построить систему привлечения клиентов и зарабатывать на ней. Агрессивно рекламируют свои услуги

В-третьих, старайтесь принимать взвешенные финансовые решения, не поддавайтесь эмоциям, повышайте свои знания в области финансовой грамотности.

Признаки пирамиды

Не поддавайтесь на агрессивную рекламу «лёгких и быстрых денег». Прежде чем принять решение о вложении денег, проверьте поступившее вам предложение на признаки финансовой пирамиды:

- Призыв не раздумывать и вкладывать быстро
- Обещание сверхвысокой доходности больше 20% годовых
- Объяснение такой доходности непрозрачными сверхприбыльными проектами
- Обещание вознаграждения за приведенных клиентов
- Анонимность организаторов и отсутствие защиты прав вкладчика в договоре
- Отсутствие информации о возможны рисках
- Требование , например, оплатить «вступительный взнос», «обучение», «участие в семинаре»
- Отсутствие лицензии/ указание номера чужой лицензии, или собственной, но не позволяющей работать с денежными средствами

Что делать

Перед тем, как отдать деньги:

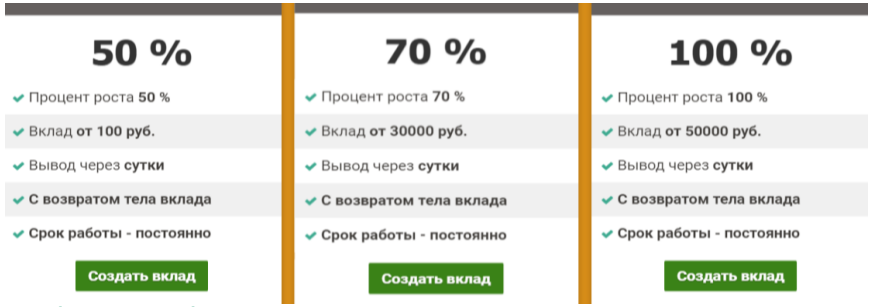
- Проверьте наличие лицензии Центрального банка на ведение деятельности (банковская, страховая, инвестиционная).
- Внимательно изучите договор на предмет условий инвестирования и возврата средств.
- Найдите в Интернете информацию о данной организации, ее историю, отзывы клиентов, рейтинги в соответствующей отрасли.

Если деньги уже вложены в сомнительные проекты, постарайтесь максимально оперативно изъять не только полученную прибыль, но и основные вложения. Не ждите, когда пирамида развалится, и не старайтесь компенсировать убытки, вкладывая новые средства.

Современная цифровая среда: риск вложить деньги в финансовую пирамиду с мобильного или с компьютера

Типы пирамид

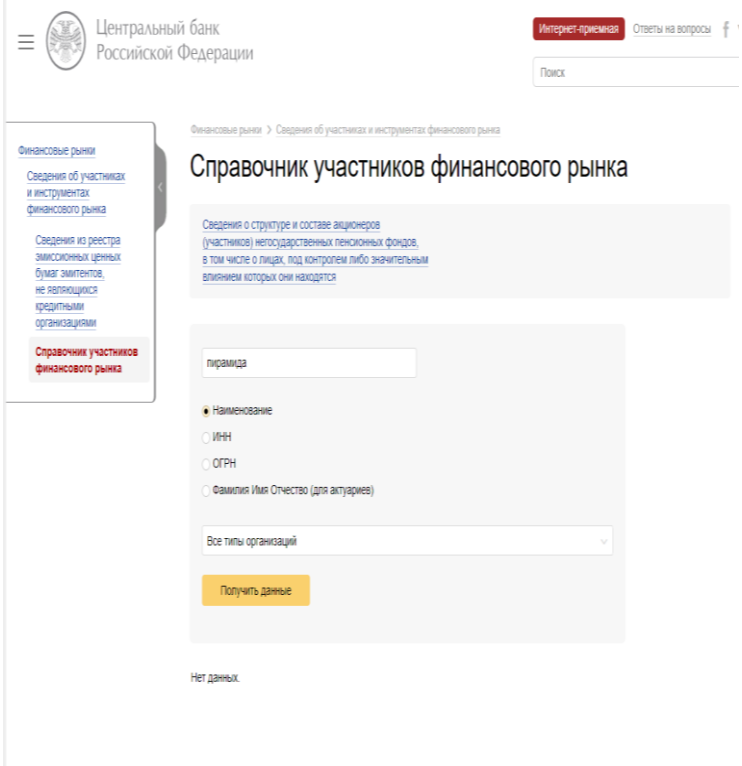
- Классические проекты, организованные на принципах сетевого маркетинга
- Проекты, работающие под видом микрофинансовых организаций, кредитно-потребительских кооперативов и ломбардов.
- «Псевдопрофессиональные участники» финансового рынка
- Проекты, позиционирующие себя как альтернатива кредитованию.
- Проекты, предлагающие финансовые услуги по рефинансированию кредитных задолженностей.
- Замаскированная финансовая пирамида — пирамида с добавлением маскирующего элемента – продукции, услуг, кэшбека



вашифинансы.рф

На сайте заманчивое предложение. Не упущу ли свою выгоду? Как проверить:

Шаг 1. Выяснить официальное наименование организации	отсутствует	Опасность!!!
	есть	
Шаг 2. проверить наличие организации на сайте ЦБ РФ (cbr.ru)	отсутствует	Опасность!!!
	есть	
Шаг 3. самостоятельно или с помощью финансовых консультантов оценить риски инвестирования	высокие риски	
	низкие риски	



Форекс бывает разным

Форекс (Forex) — это международный межбанковский рынок обмена валюты.

Часто в СМИ и в интернете встречается реклама финансовых посредников, так называемых дилинговых организаций, предлагающих населению принять участие в спекулятивной игре на Форексе. В такой рекламе может говориться о перспективе заработать с их помощью целое состояние. Приводятся примеры успешных людей, сделавших состояние на рынке Форекс. В случае проигрыша любезно рекомендуются платные образовательные программы профессиональных трейдеров, инвесторов.

В действительности клиенты дилинговых компаний самостоятельно не совершают операции на международном рынке.

Схема работы

Компании, предлагающие услуги на рынке Форекс, в основном получают доход от кредитования (предоставления займов) своих клиентов — физических лиц. Такие кредиты обычно называются «плечами». В связи с этим главной задачей дилинговых компаний является предоставление **кредитного плеча** (рассчитываемого как отношение суммы сделки к собственным средствам), величина которого может достигать 1/100.

То есть на каждый рубль собственных средств можно совершать сделки на 100 рублей.

Такое кредитное плечо преподносится в рекламе как возможность много заработать с минимальной суммой собственных денег). Но как любое плечо (рычаг), оно работает в обе стороны. Так, при наличии кредитного плеча, равного 100, движение рынка против игрока всего лишь на 1 % означает **полную потерю им 100 % собственных средств**!

С учетом того, что среднее движение валютных курсов равно примерно 1 % в сутки, **вероятность потерять свои средства за два месяца приближается к 99 %**. При этом сама дилинговая организация независимо от того, получит ее клиент прибыль или понесет убыток, всегда успеет в результате проводимых спекуляций получить свои проценты.

Риски сотрудничества

Получение клиентом крупной прибыли может иметь криминальные последствия: возможны разнообразные махинации, в том числе организация различных технических сбоев и совершение несанкционированных операций по счету клиента.

Если человек соглашается сотрудничать с кем-то из посредников, действующих на этом рынке, все риски он берет исключительно на себя.

Деятельность подобных Форекс-компаний начинает регулироваться Центральным банком России. Но какие бы меры ни принимало государство, оно не способно полностью защитить частных инвесторов от риска быть втянутыми в различного рода мошеннические схемы на финансовых рынках, если они сами не заинтересованы в этом. Прежде всего граждане должны обладать хотя бы минимумом финансовых знаний и проявлять должную осмотрительность при выборе инструментов для вложения своих сбережений.

Резюме

- Проявляйте бдительность и внимательность к своим ежедневным финансовым операциям.
- Никогда никому не сообщайте ваши пароли, ПИН-код, CVV.
- Используйте антивирусное программное обеспечение.
- При совершении платежей в интернете обязательно проверяйте, какой URL стоит в адресной строке
- Не передавайте банковскую карту третьим лицам.
- Обязательно установите пароль для разблокировки телефона, особенно если на нем установлено банковское мобильное приложение.
- Гарантирование доходности по инвестициям, в несколько раз превышающей рыночный уровень, является признаком финансовой пирамиды.
- При получении сомнительных СМС от банков или лиц, представившихся родственниками, позвоните в банк или родственникам, уточните информацию. Не отвечайте на сомнительные СМС.
- Если Вы стали жертвой финансовых мошенников, сообщите в полицию.

Медицинские услуги в кредит

Телефонный звонок или врученный на улице подарочный сертификат с предложением воспользоваться акцией с бесплатными ознакомительными процедурами или диагностикой в медицинских центрах — не каждый человек способен понять, что речь идет о ловушке.

Нередко пациент приходит в центр, где попадает в руки нечистоплотных дельцов. Итогом таких мероприятий, как правило, становятся кредитные договоры на медицинские услуги, зачастую не только бесполезные, но и противопоказанные.

Спустя время, когда человек понимает, что ему навязали кредит в медицинском центре — на кругленькую сумму и с внушительными процентами, возникает естественное желание — отказаться от дорогостоящих услуг. Как быть?

Медицинские услуги в кредит. Как расторгнуть договор с медицинским центром

В соответствии с законодательством Российской Федерации, можно в одностороннем порядке отказаться от услуг или выполнения работ, подав уведомление в клинику с требованием вернуть полученную сумму за услуги в банк.	Если деньги уже были выплачены Мед. Организация, обязаны вернуть уже полученные деньги, удержав из возвращаемой суммы расходы за пройденные процедуры.
Пациент вправе ознакомиться с прейскурантом на конкретные услуги, потребовав подтверждающие документы.	Стоит учесть, что срок возврата денежных средств законодательно не регламентирован, поэтому пациент может, исходя из положения ст. 314 ГК, потребовать возврата денег в 7-дневный срок с момента получения центром уведомления.
Также следует незамедлительно обратиться в банк с заявлением о расторжении договора медицинских услуг, кредит в котором был оформлен. Необходимо указать дату и номер договора, сопроводив просьбой не перечислять на счет центра сумму, указанную в договоре, если деньги еще не были перечислены. Отказ от получения кредита лучше оформить не позднее даты одобрения договора банком. Если кредит уже одобрен, погашать его придется.	
Если же за навязанный кредит в медицинском центре денежные средства банком уже перечислены, следует, прежде всего, направить в медучреждение заявление о расторжении договора на оказание медуслуг с требованием о возвращении всех денежных средств.	Помните, если своевременно деньги не будут возвращены медицинским центром, вернуть кредит пациенту все равно придется. Причем условия выплаты лучше не нарушать, иначе штрафы придется платить за свой счет.
Также можно подать заявление в Центробанк, описав обстоятельства заключения кредитного договора и акцентировав внимание на одобрение кредита без оценки платежеспособности пациента, без предоставления ему доверенности на правомочие заключения сделки и др. — оформление кредита в подобных условиях является нарушением.	
Если же реакции от медицинского центра не последовало, можно подавать жалобу в Роспотребнадзор на деятельность Мед. Организации и банк, оформивший данный кредит, описав все обстоятельства его выдачи.	
Если эти обращения оказались также безрезультативными, вопрос придется решать в судебном порядке.	

ВСЕРОССИЙСКАЯ НЕДЕЛЯ СБЕРЕЖЕНИЙ

Оценка полезности

Тест

Тест

1. Как можно сделать использование банковской карты максимально безопасным:

- Никогда не сообщать третьим лицам PIN/CVV/CVC-2 код, в том числе и сотрудникам банка
- Отправлять фотографию карты с двух сторон тем, кто хочет перевести мне деньги
- Подключить СМС-информирование, чтобы точно знать, когда происходит операция по карте
- Сообщать посторонним лицам одноразовый пароль, который приходит по СМС
- Заблокировать карту при обнаружении ее пропажи
- Написать ПИН-код непосредственно на карте, чтобы не забыть его и случайно не заблокировать карту

2. Как безопасней оплачивать товары и услуги через сеть:

- С помощью своей зарплатной карты, чтобы заработать дополнительные бонусы
- С помощью кредитной карты
- С помощью специальной карты для покупок в Интернете

Тест

3. Что не является финансовым мошенничеством?

- Вам сообщают, что вы выиграли приз и просят вас внести регистрационный взнос за выигрыш
- Центральный банк РФ сообщает вам, что ваша банковская карта заблокирована
- Сотрудник банка просит вас назвать PIN-код вашей банковской карты
- При обращении вами в колл-центр банка, вас просят назвать кодовое слово или паспортные данные
- Все описанные ситуации являются мошенничеством

4. Перечислите способы защиты от интернет-мошенников:

- Никогда и никому не сообщать пароли
- Сообщать пароли только сотрудникам банка
- Никогда не делать копий файлов с секретной информацией
- Не открывать сайты платежных систем по ссылке (например, в письмах)
- При поиске удаленной работы не реагировать на просьбы оплаты каких-либо регистрационных взносов

Тест

5. Друг приглашает вас и еще несколько человек поучаствовать в новом инвестиционном проекте, который вкладывает в высокодоходные бизнесы в Европе / за рубежом. Ваше решение:

- Буду участвовать, я доверяю словам друга
- Буду участвовать, поскольку бизнес в Европе надежнее, чем в России
- Выясню подробности о данной организации, наличие у нее лицензий, договора и только после этого приму решение
- Буду изучать возможности и риски и посоветуюсь с разными специалистами

6. Вы вложили средства в надежде получить высокую доходность, но выяснили, что организация по всем признакам похожа на финансовую пирамиду. Каковы ваши дальнейшие действия?

- Максимально быстро заберу все вложенные средства, даже ценой потери потенциального дохода
- Рискну и оставлю все вложенные деньги
- Внесу еще денег и приглашу знакомых для участия в надежде поддержать устойчивость пирамиды

Тест

7. Как называется вид мошенничества, предполагающий установку специальных устройств на банкоматы, с помощью которых преступники получают информацию о карте?

- Ливанская петля
- Фишинг
- Скимминг

8. На сайте незнакомой вам финансовой компании в Интернете вы увидели выгодное предложение о размещении денег под 25 - 36% и более годовых (или 2 - 3% и более в месяц). Какова вероятность того что данная организация является финансовой пирамидой?

- Низкая, поскольку они гарантируют возврат денег и доходность
- Средняя, поскольку доходность высокая, а значит и риски тоже высокие
- Высокая вероятность, поскольку такая доходность в современных экономических условиях не может быть гарантирована

Тест

9. Какие из утверждений верны:

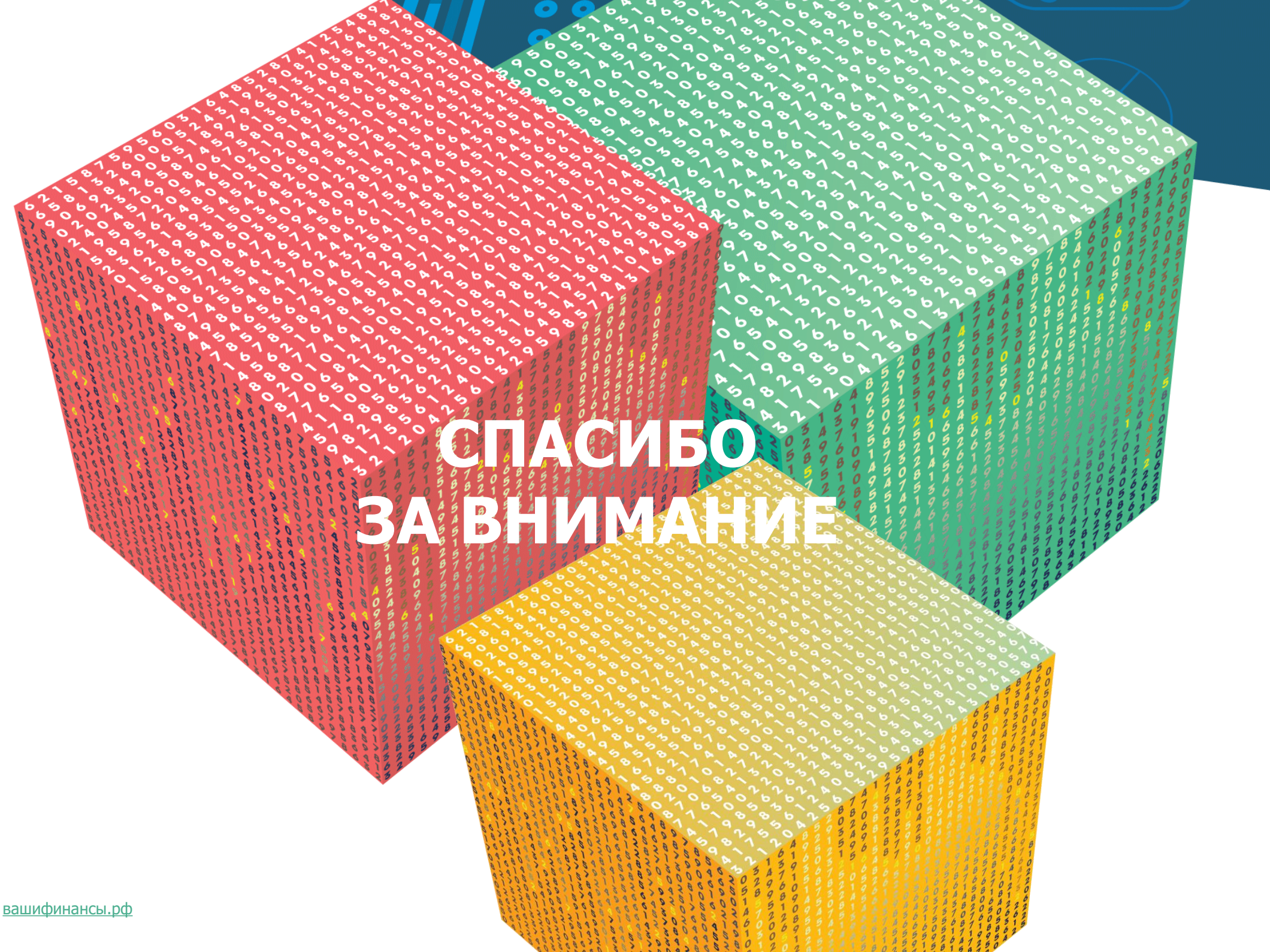
- Форекс (Forex) – это международный межбанковский рынок обмена валюты
- Существуют компании (финансовые посредники), которые предлагают населению принять участие в спекулятивной игре на Форексе
- Центральный Банк РФ ответственен за все риски потери капитала при работе граждан с Форекс-компаниями
- Все вышеперечисленное

Хотите научится принимать грамотные финансовые решения?

Регистрируйте на бесплатный онлайн курс по ссылке:
www. course.ncfg.ru

Получайте надежную и комплексную информацию по финансовой грамотности, не выходя из дома. Программа разработанную в рамках проведения Всероссийской недели сбережений.

После прохождения всего курса –распечатайте именной сертификат!



СПАСИБО ЗА ВНИМАНИЕ

вашифинансы.рф