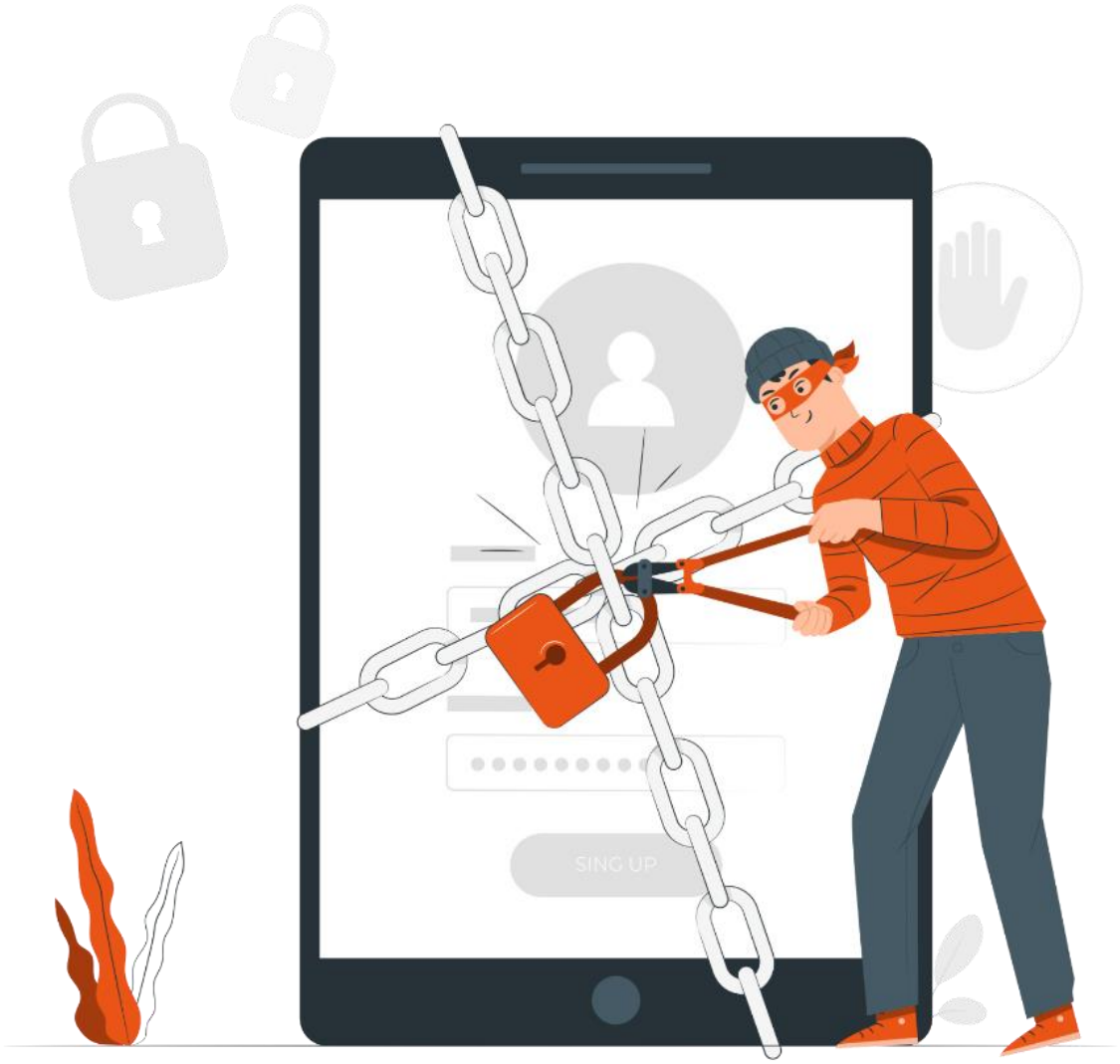



# Что такое хорошо и что такое плохо

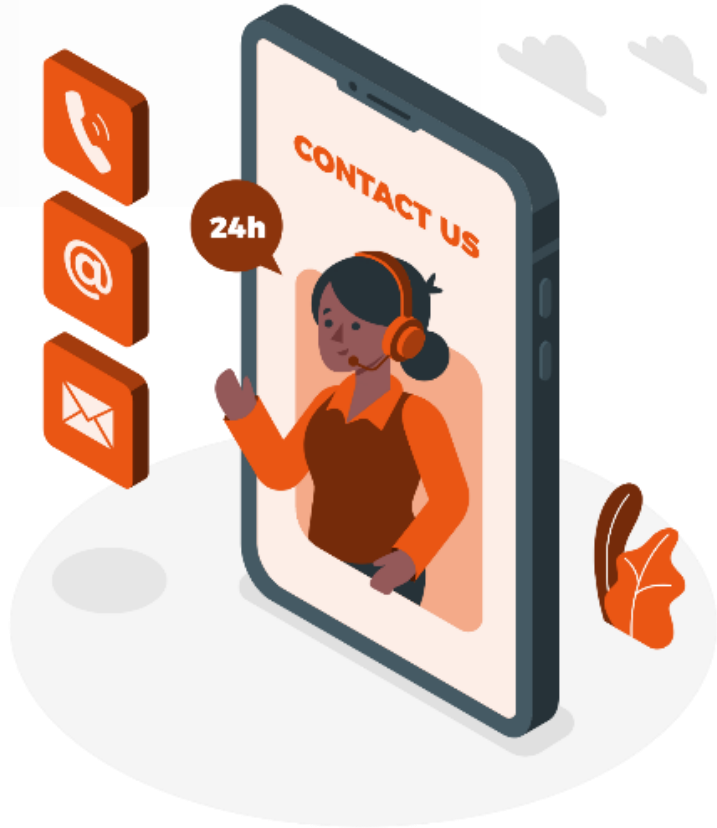
## Как защититься от кибермошенников

Каратун Артём Сергеевич +7 961 097 94 54
Перцева Екатерина Александровна +7 983 053 03 72

ПСБ

psbank.ru

# Телефонное мошенничество

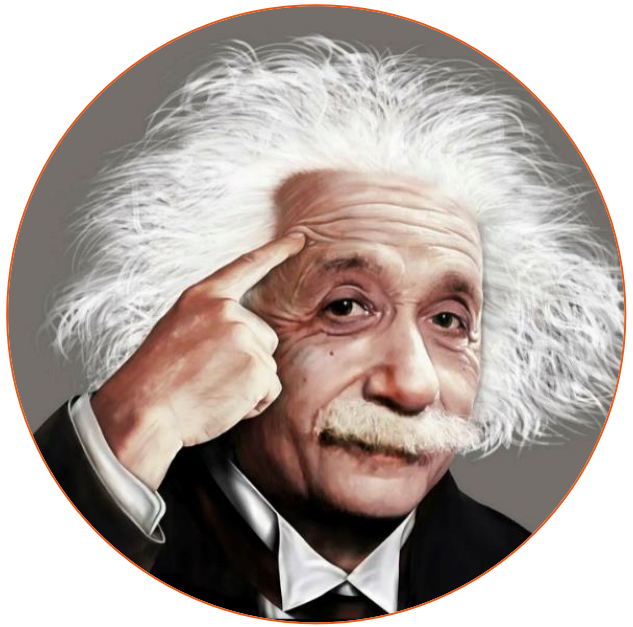


Верно ли утверждение:

при обнаружении мошеннических операций надо первым делом обратиться в полицию с заявлением о краже денежных средств?

# Почему же это работает?

СТРАХ и АЛЧНОСТЬ – две из трех движущих сил человеческого поведения, который Эйнштейн называл Великими (третьей была глупость).



## Как строят диалог мошенники

Использование лично значимых угроз

Предложение простого и эффективного решения

Призыв к действию сразу после успокаивающего сообщения

Поддерживающие слова подтверждающие, что это верный шаг навстречу лучшему, после того как клиент ответит на призыв

# Перевод на «безопасный счет»


Звонок клиенту, представляясь сотрудниками «Службы безопасности» и сообщение о попытке совершения операции по его карте:

“Ваши средства находятся в опасности. Для исключения возможности финансовых потерь необходимо перевести сбережения на безопасную ячейку *якобы открытую на ваше имя.  Это можете сделать вы сами или предоставить свои данные (номер карты, код из СМС) “сотруднику службы безопасности” для совершения перевода.


*Данной «ячейкой» может являться счет физического лица, счет юридического лица, индивидуального предпринимателя, карты ПСБ и других банков.

Часто пострадавшие закрывают все свои вклады, используют кредитные средства (карты, кредиты). Также клиент может провести операцию снятия наличных в АТМ и взнос на «безопасный счет».

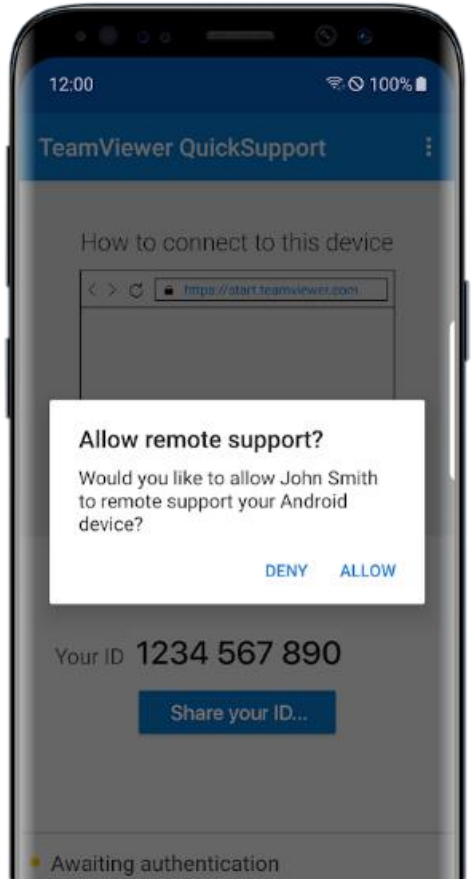
# Использование программ удаленного управления

Звонок от сотрудника «Службы безопасности» и сообщение о попытке совершения операции по его карте.

**1** Клиента убеждают установить на мобильное устройство приложение удаленного управления (в недавнем прошлом Quick Support, сегодня, в основном AnyDesk) и разрешить подключение к устройству «сотруднику банка».
Чаще всего предлогом для установки бывает удаление вирусов с устройства клиента, помощь в спасении средств клиента.

**2** В случае если устройство позволяет проводить операции удаленно, злоумышленники просят зайти в мобильное приложение и проверить сохранность средств, а затем перевернуть устройство и подождать, пока «сотрудники банка» удалят вирусы.

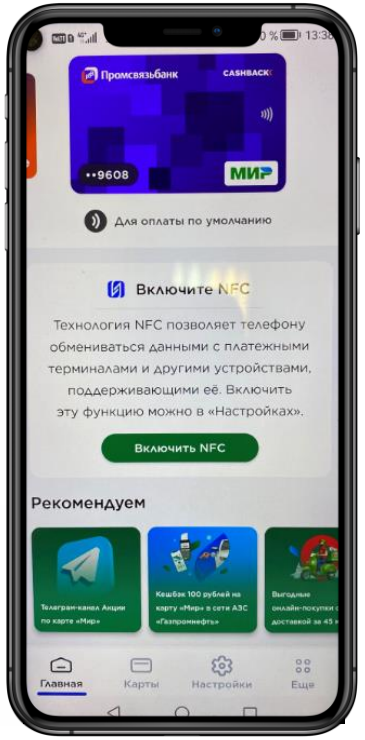
**3** В это время злоумышленники проводят списания через мобильное приложение клиента.
Если мобильное приложение не позволяет проводить удаленное управление через Quick Support, а только транслировать экран, злоумышленники убеждают клиента перевести средства на «безопасный счет».



# Токенизация карты

**1** Звонок клиенту от сотрудника «Службы безопасности» и сообщение о попытке совершения операции по его карте

**2** Для спасения денежных средств клиента убеждают “выпустить новую карту” На самом деле клиент токенизирует у себя на устройстве карту мошенников




**3** Для успешной токенизации клиенту сообщают одноразовый пароль (он приходит мошенникам, так как токенизируется их карта)

**4** Далее клиента убеждают снять все деньги со счетов и внести их на новую карту через банкомат используя токен

# Письма несчастья вместо звонка

Фальшивый документ с поддельными подписью и печатью на бланке кредитной организации. Такое письмо могут отправить как по электронной почте, так и по обычной.

Формулировки могут варьироваться, но суть неизменна: в письме будет указан номер счёта, на который нужно перевести деньги.

В тексте письма будет сказано, что вы стали жертвой мошеннических действий и для обеспечения безопасности нужно «выполнить процедуру обновления единого номера лицевого счёта».

Письмо содержит персональное обращение с указанием имени, отчества и фамилии.


Банк России

Исх. № 63462740 По месту требования

Документ № 62457203

Центральный Банк Российской Федерации настоящим письмом уведомляет, что Вы, Трофимов Владимир Григорьевич, стали жертвой мошеннических действий. Для обеспечения безопасности финансовых активов, согласно договора банковского обслуживания, необходимо выполнить процедуру обновления единого номера лицевого счёта.
Ниже представлены Ваши действующие реквизиты:

Обеспеченный счёт: 40819685134827596752
Срок действия обновленных реквизитов составляет 24 часа.

Специалист финансового отдела: Жуков Максим Романович

* Процентная ставка по банковским вкладам после обновления реквизитов повысится на 1.5% годовых.
* После обновления реквизитов все финансовые активы, которые находились на счетах клиента до мошеннических действий будут восстановлены.

Банк приносит свои извинения за сложившуюся ситуацию. Мы сделаем все для того, чтобы в дальнейшем Вы не оказались в подобной ситуации.

Реквизиты банка:
Банк: Филиал №3 ЦБ РФ г. Москва
БИК: 044536002
ИНН: 7702235133
Корр.сч.: 30101810400000000138

Зам. Начальника ОПНО ГУ по Москве и филиала №3 ЦБ РФ
М.П.

А.М. Калиниченя

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Необходимо помнить: перевести ваши деньги на другой счёт под предлогом их спасения предлагают только мошенники, ПСБ так никогда не поступает.

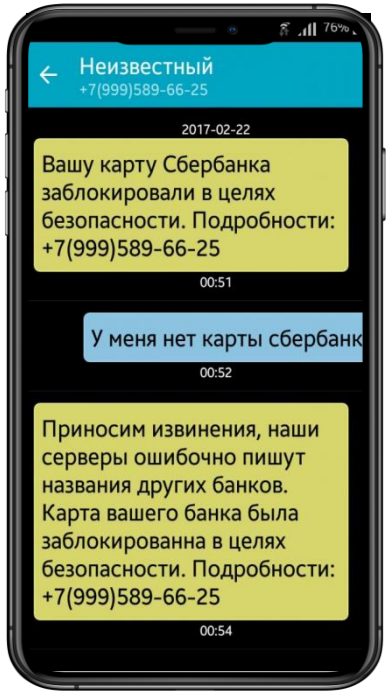
# Разнообразие тем телефонного мошенничества

Звонок из Генпрокуратуры – примите участие в расследовании

Голосовой помощник – сообщите смс-код

Звонок из Службы безопасности…

С Вашего счета хотят перевести деньги в другом городе…




Помогите поймать нечестного сотрудника…

Продиктуйте код для отмены мошеннической операции…

Звонок робота – карта заблокирована, перезвоните, пожалуйста по номеру….

На вас оформили кредит…

# Как защитить себя от телефонного мошенничества

- Внимательно проверяйте входящий номер (звонок через мессенджер=мошенники)
- Не совершайте никаких операций по инструкциям звонящего.
- Работник банка никогда не попросит у вас CVV/CVC-код, логин, пароль от мобильного банка или коды из СМС. Если услышали такую просьбу сразу заканчивайте разговор.
- Проверьте, не было ли сомнительных операций за время разговора. Если успели что-то сообщить мошенникам, сразу позвоните в банк на номер с оборотной стороны вашей карты и сообщите о случившемся.

Неверно:
прежде всего необходимо заблокировать карту любым доступным способом

# SMS мошенничество

Верно ли утверждение:
99% мошеннических рассылок направлены не на одного конкретного клиента, а на множество адресов?

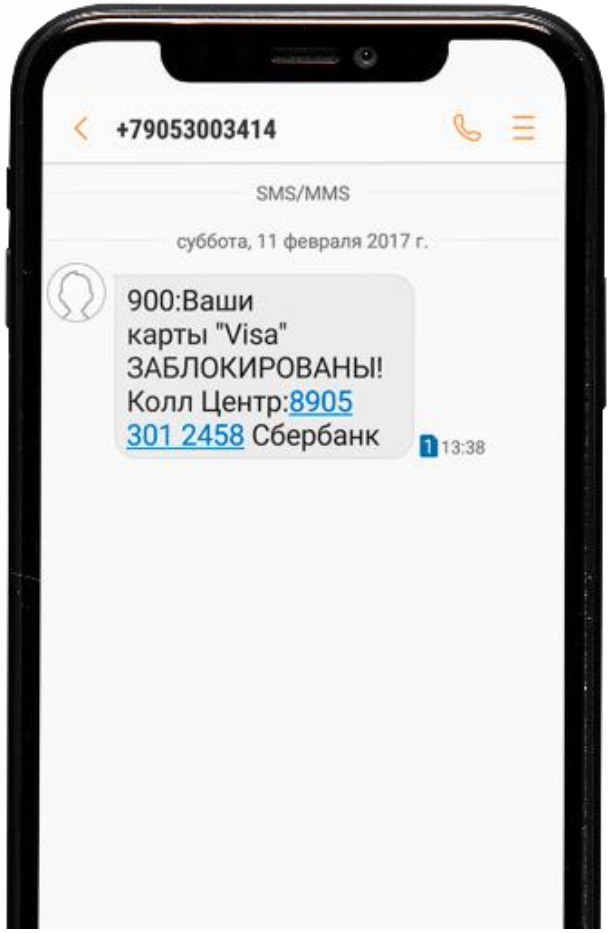
# Срочно следуйте инструкциям...

Веерная SMS-рассылка по номерам телефонов. Наиболее распространены варианты сообщений – о блокировке карты или о совершении операции по карте. В сообщении указан телефон, по которому клиента просят перезвонить.

Представляются:

- сотрудниками «Службы безопасности»
- специалистами службы технической поддержки;
- менеджером контактного центра;
- сотрудниками платежной системы и пр.

В убедительной форме предлагают срочно провести действия по разблокировке карты, по отмене перевода и т.п. Клиенты выполняют получаемые по телефону инструкции.



# СМС имитация реальных услуг банка

## Заказ онлайн через сайт банка

На сайте Банка выбирается любая карта, «заказ онлайн», «оформить онлайн», вводят произвольные данные мошенников и телефон клиента-жертвы. СМС-пароль для подтверждения операции приходит клиенту

## Смена номера телефона

или других реквизитов

## Вход в «Свой Бюджет»

СМС для входа может приходить по любому из сервисов ПСБ. Эта попытка (реальная СМС на ваш номер) используется как предлог для гипноза клиента мошенниками

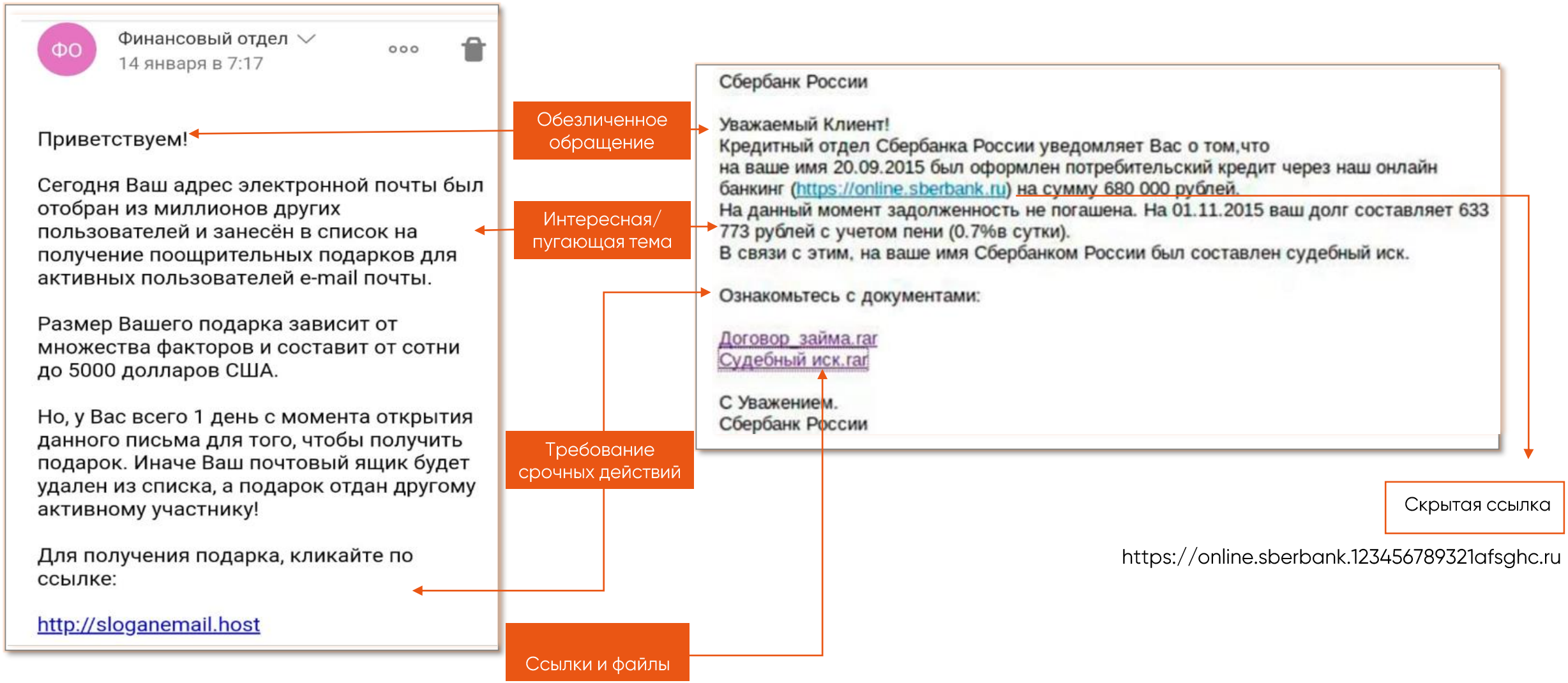
SMS86 Nikomu ne govorite etot kod, ego sprashivayut tol'ko moshenniki. Dlya vhoda v lichnyj kabinet vvedite kod 374765 . Vash PSB: 88003330303

## Подмена текста

сообщения при использовании внешних сайтов (Авито, Юла и др.)

# Фишинговые письма

# Как понять, что письмо фишинговое



# Как защитить себя от фишинговых писем

1. Обращайте внимание на домен. Мошенники обычно используют общедоступные почтовые домены gmail.com, mail.ru и т.п. или покупают домены, похожие на официальные имена компаний, чтобы ввести получателя в заблуждение.

2. Вас должно насторожить, если тема, контент письма или название файлов побуждают вас к немедленному действию.

3. Обращайте внимание на обращение и подпись. Если они являются безличными или есть признак автоподстановки в обращении, то высока вероятность фишинга.

4. Не переходите по ссылкам, не кликайте на подозрительные объекты. Наведите курсор мыши на подозрительную ссылку/объект и вы увидите, куда она ведёт на самом деле. Сравните её с официальным сайтом компании.

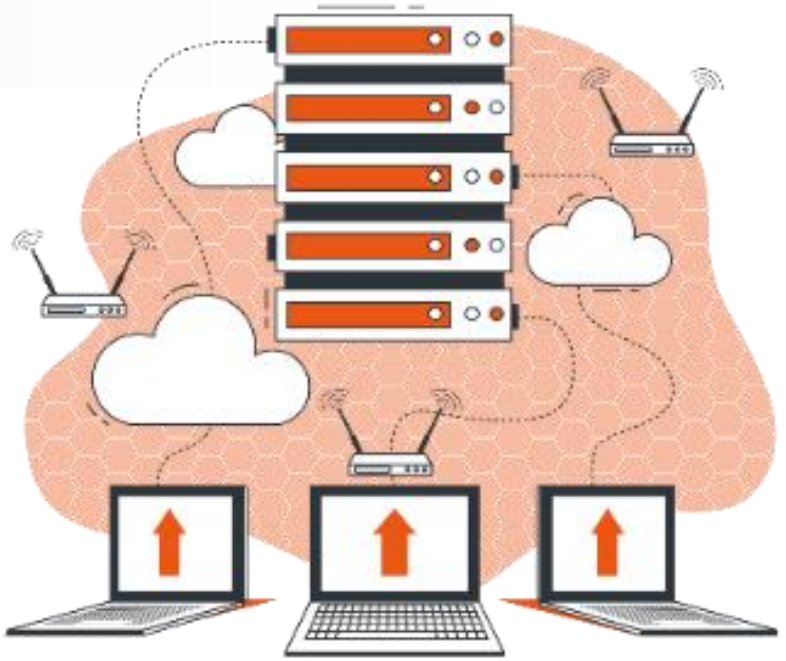
5. Будьте осторожны с вложениями, открывайте только те, которые ждали.

6. Не вводите свои данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы.

7. Не отвечайте на подозрительные письма.

**Верно:**
таргетированные атаки встречаются, но основная масса рассылок веерные, так как мошенникам вполне достаточно одного сотрудника, открывшего вредоносное письмо

# Мошенничество в сети Интернет



Верно ли утверждение:
Файлы cookies сохраняют только историю наших действий на сайте

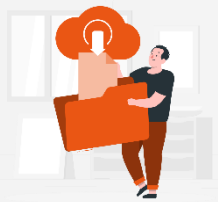
# Что знает о нас интернет:

## Интернет-магазины

- Предпочтения
- Платежная информация
- Физические параметры (размеры обуви и одежды)

## Социальные сети

- Друзья и знакомые
- Политические и религиозные убеждения и активности
- Хобби



## Службы доставки

- Место жительства и работы
- Уровень дохода

## Такси и каршеринг

- Время и маршруты поездок

## Билеты

- Данные о перелётах, поездках и попутчиках


## Поисковые системы

- История запросов
- Действия на сайте
- Выбор товаров и услуг
- Идентификаторы устройств
- Файлы cookie
- Данные об учетных записях

## Государственные услуги

- Паспорт и другие документы
- Состав семьи
- Состояние здоровья

## Карты и навигаторы

- Местоположение и передвижения
- Любимые места
- Модели поведения

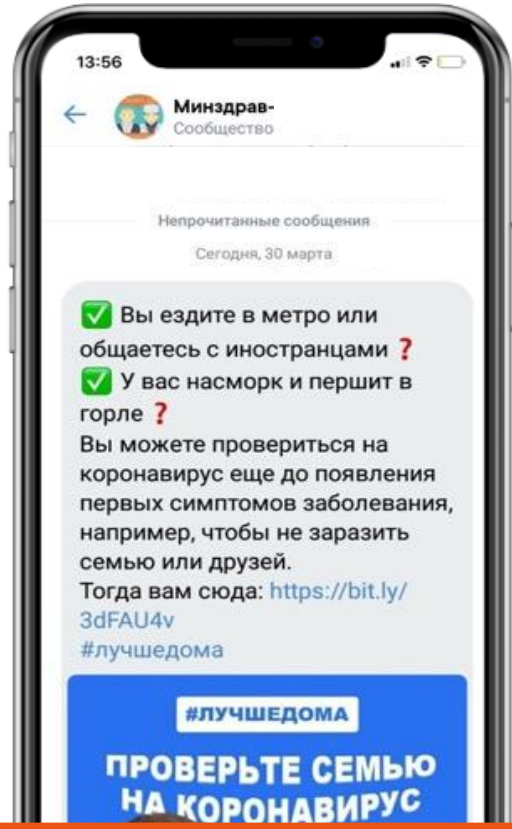
# Компрометация реквизитов карты через фишинговый сайт

1. Злоумышленники создают в сети Интернет фишинговые сайты для сбора персональных данных клиентов.

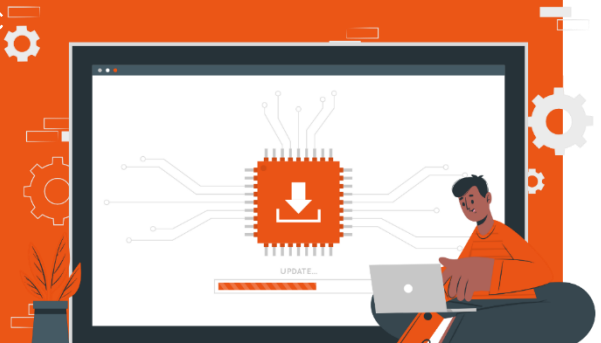
2. Клиент заходит на фишинговый сайт и вводит данные своей банковской карты.

3. Мошенник, получив данные карты клиента, совершает покупки в интернет-сервисах, не поддерживающих технологию оплаты с подтверждением одноразовым паролем.

4. Операции списания в основном выполняются с помощью бота.




Пример:
Проверь себя и свою семью на коронавирус



# Покупка в Интернет по выгодной цене (часто сезонные акции)

1

Мошенники создают поддельный сайт или размещают объявление о распродаже товаров известных брендов в социальной сети

2

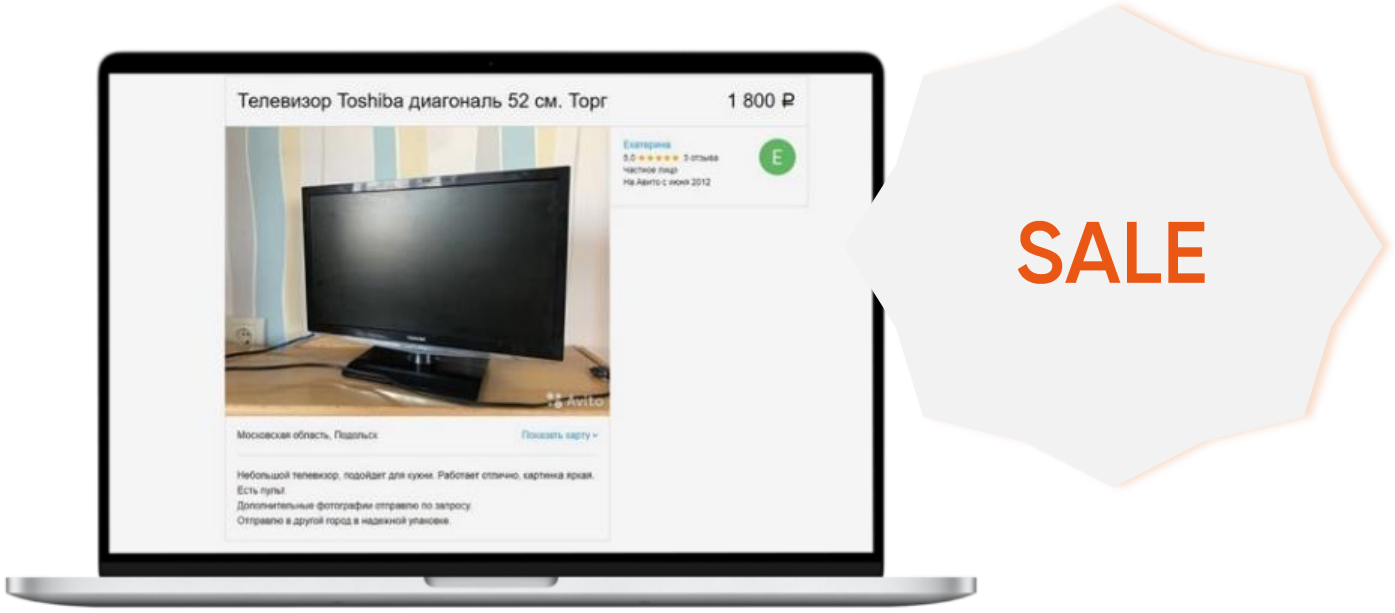
Клиент желая приобрести популярные товары по более дешевой цене осуществляет заказ или покупку

3

Покупатель осуществляет перевод денежных средств в пользу неизвестных

4

После внесения предоплаты продавец перестает отвечать на звонки и сообщения от покупателя



# Торговля из рук в руки / доски объявлений

При продаже товара у вас просят данные карты для перевода вам оплаты за товар

Помните, что одноразовые пароли приходят только на расходные операции и диктовать их нельзя.
Если вы получили пароль, то деньги у вас пытаются списать, а не зачислить.

Если  все-таки произошло списание, которого вы не ожидали, то не пытайтесь отменить операцию, продолжая общение с «покупателем» на сайте

Необходимо прекратить разговор и обратиться в банк, в противном случае Вы снова отправите денежные средства мошенникам.


Если вам предлагают оформить доставку

Не переходите по ссылке, которую вам присылает покупатель - это фишинговая ссылка.
Часто для этого используют мессенджер (например, WhatsApp), куда вас приглашают продолжить диалог.

# Фиктивные опросы/выплаты/компенсации


Сайт с использованием символики официальных органов РФ, обещающий крупное вознаграждение или помощь в получении выплат/компенсаций. Под различными предлогами клиента убеждают провести оплату за услуги, связанные с оформлением вознаграждения/выплаты/компенсации.


На сайте необходимо пройти регистрацию, чтобы найти вас в системе. Далее сообщают о крупном выигрыше или возможности получения солидной компенсации.

Для получения денежных выплат клиент самостоятельно проводит оплату услуг специалистов, якобы помогающих в оформлении документов.

# Как защитить себя от мошенничества в интернете

1. Не сообщай номер своей банковской карты, срок действия, CVV-код и код из СМС

2. Как правило, со всеми акциями банков можно ознакомиться на их официальных сайтах и страницах в социальных сетях. Если вы не нашли предлагаемую активность на официальных ресурсах, откажитесь от участия

3. Если для получения большой суммы денег вам сначала предлагают потратить сравнительно небольшую, будьте осторожны, это мошенничество

4. Рекомендуется завести несколько адресов электронной почты, например: частный – для личной переписки публичный – для открытой деятельности в социальных сетях и т.д.

5. Отправляя кому-либо личную информацию, убедись в том, что адресат – действительно тот, за кого себя выдает

# Мошенничество в социальных сетях

# Как «утекают» ваши персональные данные

В пользовательских соглашениях популярных соцсетей есть пункты, которые гласят:

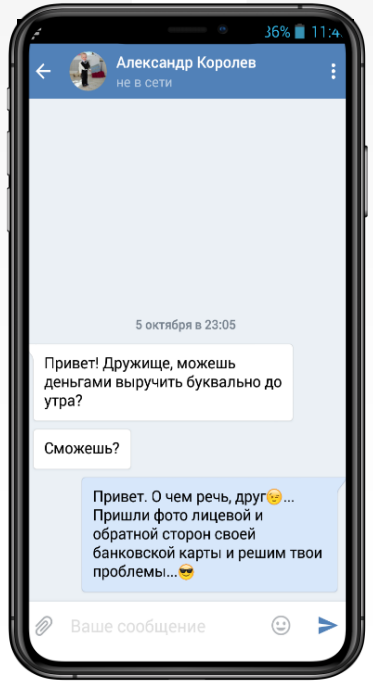
«Мы делимся вашими данными с нашими сторонними поставщиками услуг, которых мы используем, чтобы предоставлять вам доступ к Платформе. Мы также предоставляем вашу информацию нашим деловым партнерам, рекламодателям, операторам аналитических и поисковых систем».

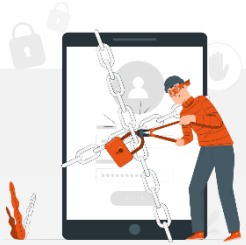
«Администрация Сайта считает, что Пользователь осознает, что информация на Сайте, размещаемая Пользователем о себе, может становиться доступной для других Пользователей Сайта и пользователей Интернета, может быть скопирована и распространена такими пользователями»

При размещении данных на сайте вы фактически теряете контроль за их использованием и распространением

# Взлом аккаунта

- Сообщение в социальных сетях со взломанного аккаунта родственника/друга.
- В сообщении просят перевести деньги или сообщить номер карты и пароли, чтобы вывести деньги с платежных инструментов (например, интернет-кошельков).
- Деньги нужны попавшему в беду близкому человеку, чтобы оплатить билет на самолет, залог или медицинское обслуживание, взятку за урегулирование проблем при аварии.



Варианты развития событий:

1. Клиент направляет деньги, после чего узнает, что аккаунт взломан.
2. Клиент разглашает запрошенные данные, после чего мошенник регистрируется в личном кабинете клиента и совершает неправомерные списания.

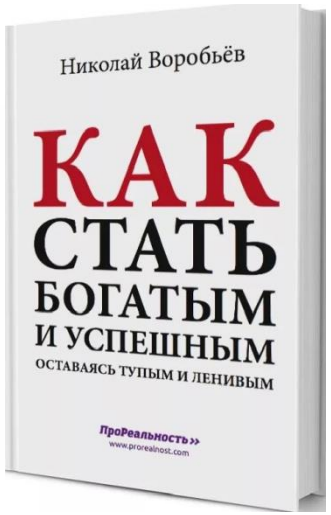
# Бизнес партнер

Мошенники создают фейковую страницу якобы успешного бизнесмена, который во всех красках демонстрирует свою роскошную жизнь

Всем, кто хочет также, «предприниматель» предлагает вложиться в его проект гарантирующий высокий доход, когда наберется достаточно средств инвесторов для начала работы

Особые условия обычно действуют «только 24» часа и количество мест «строго ограничено»

После вложения денег инвестор попадает в черный список, а аккаунт бизнесмена исчезает



# Опасные предложения

- Хакеры предлагают сотрудникам российских компаний открыть доступ к внутренним данным или запустить вредоносный код

- За подобные действия мошенники предлагают достаточно крупные вознаграждения

Если вам поступило  такое предложение, лучше от него отказаться, так как за содеянное предусмотрена административная и уголовная ответственность!

# Осторожно, скаммеры!

**1** Под видом романтических отношений: знакомства через Интернет, социальные сети, службы подбора «невест по переписке», предлагают потратить средства на любимого человека:

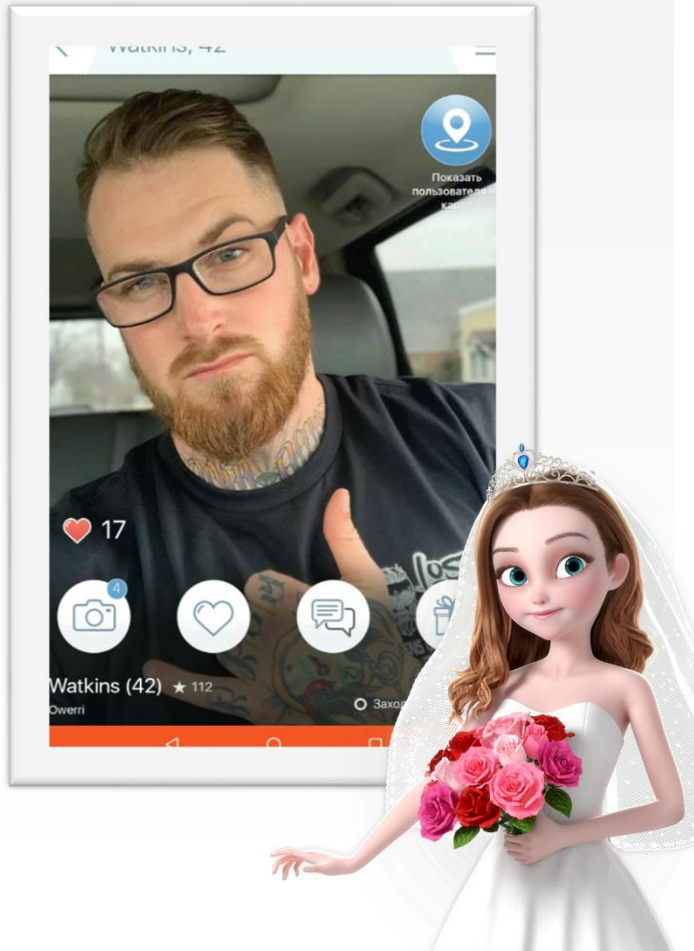
Оплатить:

- пересылку подарка,
- налоги на таможне для доставки подарка,
- переезд,
- деньги в долг

**2** После получения средств злоумышленники перестают отвечать на звонки и сообщения.

**3** Чаще всего жених и невеста проживают в разных странах.

Все схемы имеют одну цель – побудить человека к отправке денежных средств.



# Тиндер фрод или знакомства с продолжением

1. Собеседница предлагает встретиться и куда-нибудь сходить.
2. Для этого она просит выкупить недорогие/последние/желанные билеты, например, на Stand Up.
3. Затем переводит общение из Tinder в WhatsAPP, где отправляет вам ссылку на фишинговый сайт. Первая попытка оплаты билетов неудачная, а вторая в 10-ти кратном размере – удачная.
4. Также дама может посоветовать ресторан, где вам принесут “астрономический” счет, а подставные сотрудники убедят вас в обязательности его оплаты.

В основном нацелен на молодых мужчин

# Хейтинг и другие инновации

- В сети создается подставной профиль, например симпатичной девушки
- С этого аккаунта рассылаются оскорбления/провокации другим пользователям
- Жертвы в поисках информации об обидчице переходят на ее страницу
- Не найдя там ничего полезного, кликают по единственной размещенной на страничке ссылке, якобы ведущей на профиль пользователя в другой сети
- Фишинговый сайт, куда мы конечно же попадаем, имитирует стартовую страницу от известной социальной сети

# Как защитить себя от мошенничества в социальных сетях

1. Установите на свои аккаунты сложные пароли

2. Проверьте настройки устройства и приложений – что, как и куда сохраняется, передается, с чем синхронизировано. При необходимости меняем настройки

3. Не указывайте в профиле личные, не общедоступные контактные данные (номер телефона, адрес личной электронной почты)

4. Не отправляйте в личных сообщениях видео и фотографии пользователям, которых ты не знаешь в реальной жизни

5. Отправляя кому-либо личную информацию, убедитесь в том, что адресат — действительно тот, за кого себя выдает

6. В случае сомнений в личности вашего нового знакомого предложите визуальный контакт и понаблюдайте за реакцией

7. Будьте бдительны

Неверно:

Cookies собирают любую информацию о посетителе сайта, в том числе персональные данные в качестве идентификаторов

# Обман в инвестициях

# “Слила в трубу”

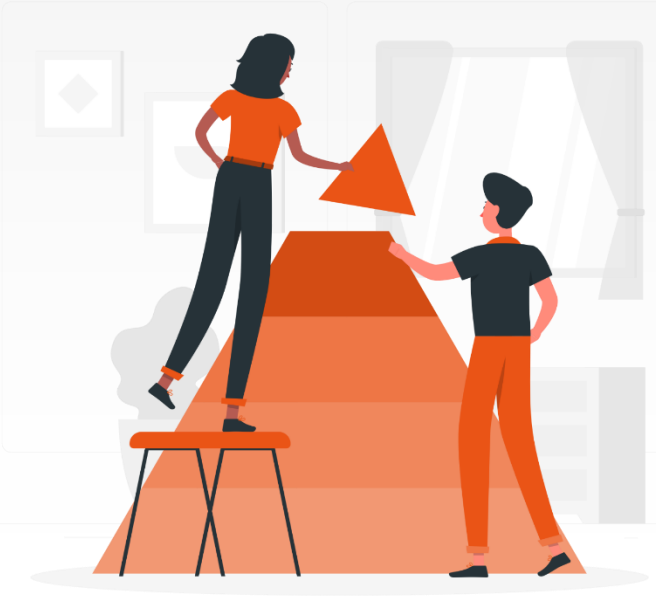
Московская пенсионерка
оформила кредит, заложила квартиру и дачу,
чтобы инвестировать 15 млн. рублей в «Северный поток – 2».
В итоге – потеряла всё.

# Финансовые пирамиды

## Признаки

- Сверхвысокая доходность, намного превышающая обычные банковские ставки по вкладам;
- Наличие обязательных предварительных взносов;
- Отсутствие информации о конкретных направлениях деятельности компании;
- В договоре с организацией отсутствуют обязательства перед клиентами при любом развитии событий;
- Максимально агрессивная реклама всеми доступными способами;
- Отсутствие лицензий на финансовую деятельность;
- Гарантии выплаты дохода, что запрещено делать легальным финансовым и кредитным компаниям.

Схема инвестиций, при которой доход первым вкладчикам выплачивается за счет средств последующих участников



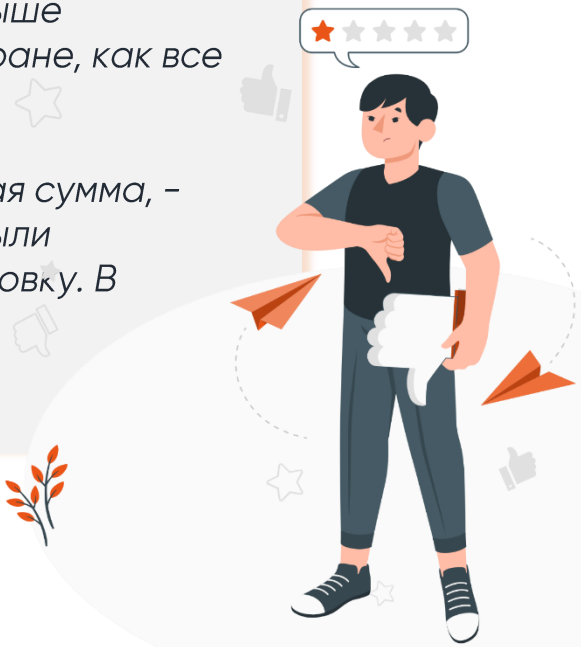
# Отзыв вкладчика инвестиционной платформы «Кэшбери»

*Я узнал о холдинге весной от брата, который уже год выводил оттуда деньги. Говорил, что уже давно отбил все свои вложения и получил чуть ли не в два раза больше. Я долго не решался, вся эта схема не внушала доверия. Но послушав брата, поверил, что получиться заработать, раз у него все вышло.*

*Деньги нужны были на семью: у меня неработающая жена и дочка. Живем к тому же в съемной квартире. Конечно, хочется чтобы условия у нас  были лучше и родные ни в чем себе не отказывали. Наверное поэтому и поверил «Кэшбери».*

*Работать с сервисом было очень просто: регистрируешься на сайте, пополняешь баланс, выбираешь подходящий тариф и инвестируешь. Тарифы отличаются по сумме вклада: чем больше денег, тем выше проценты. Первое начисление процентов происходит уже через сутки – сидишь  и смотришь на экране, как все увеличивается.*

*Вывести я ничего не успел. Сначала долго ждал подходящего момента, когда накопиться приличная сумма, - думал, что смогу снять побольше денег. Но когда дождался, все перестало нормально работать: были проблемы с переводом на карточки, кошелек замораживали, нужно было покупать какую-то страховку. В общем, тогда я понял, что денег не увижу.*



# Как защитить себя от подобных историй

1. Прежде чем переводить деньги, убедитесь, что у компании есть лицензия на осуществление брокерской или дилерской деятельности, перечень представлен на сайте Центрального банка РФ

2. Перед тем, как подтвердить платежную операцию, убедитесь, что все реквизиты указаны верно. Реальные брокерские или дилерские компании не просят перевести средства на карту третьего лица

3. Не принимайте спонтанных решений. Особенно если вам говорят: “я уже туда вложил деньги”

# На сколько мошенники “в тренде”

# Мошенники пристально следят за новостной лентой и постоянно актуализируют свои схемы

## Санкции и платежные ограничения

Например, сегодня отмечается появление фейковых виртуальных карт оплаты в App Store или PlayStation Store, мобильных приложений банков, после того как официальные сервисы исчезли из App Store и Play Market.

## Сезонные и громкие события

Перед началом отпускного сезона стали появляться мошеннические ресурсы для оплаты проезда по российским автомагистралям или на городском транспорте, приобретения «дефицитных» товаров из IKEA.

## Инвестирование

Активно развиваются схемы с «инвестированием» в криптовалюты, акции, драгоценные металлы.

# Карточный туризм

В 2022 году набирает оборот новая мошенническая схема в виде помощи с оформлением карт банков стран СНГ.

Для оформления карточки в иностранном банке клиент передает неизвестным свои персональные данные, сканы документов, доверенность и предоплату за услуги. Предоставление этих данных мошенникам несет серьезные риски.

Желающим воспользоваться услугами посредников при оформлении банковских карт, следует быть особо бдительными. Нужно обязательно проверить контрагентов на надежность, изучить отзывы о них, поскольку существует большая вероятность столкнуться с фишингом.

# Будьте бдительны!

1. Не сообщай номер своей банковской карты, срок действия, CVV-код и код из СМС
2. Не совершайте никаких операций по инструкциям звонящего
3. Не открывайте ссылки из сообщений от незнакомых номеров
4. Установите на свои аккаунты сложные пароли
5. Устанавливайте на свои устройства программное обеспечение только из официальных источников
6. Перепроверяйте все акции на официальных сайтах и страницах в социальных сетях
7. Если для получения большой суммы денег вам сначала предлагают потратить сравнительно небольшую, будьте осторожны, это мошенничество
8. Заведите несколько адресов электронной почты для разных целей
9. Не отправляйте незнакомым людям кому-либо личную информацию
10. Проверяйте настройки устройства и приложений
11. Будьте осторожны с вложениями, открывайте только те, которые ждали
12. Не вводите свои данные, логин и пароль на подозрительных сайтах или в какие-либо анкетные формы

# Если слышите такое в телефоне - смело бросайте трубку

### Продиктуйте код из СМС

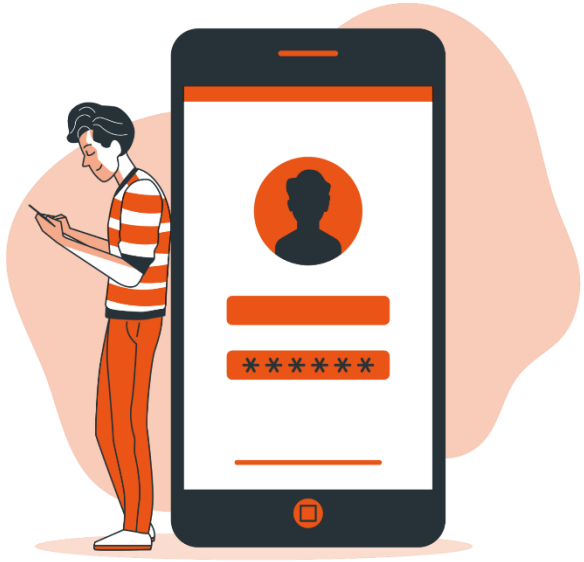
Так вы даете доступ к своему счету –
и пока-пока, деньги!

### В другом городе был совершен подозрительный перевод

Так вовлекают в «расследование», после которого со счета снимают все деньги

### Помогите поймать сотрудника

Ловушка для сторонников правосудия.
Никого не поймают, а твои деньги спишут




### Загрузите безопасное приложение

Это «безопасное приложение – пропуск для мошенников к твоему счету

### На вас оформили кредит

Для его «отмены» узнают ваши данные и оформят уже настоящий кредит ☺

### Отправьте деньги на защищенный счет

Все ваши средства будут под «защитой» мошенников!

По любым вопросам, включая безопасность ваших финансов –
обращайтесь в Банк по телефону
на оборотной стороне вашей банковской карты

ПСБ