Мошенничество с использованием методов социальной инженерии – самый распространенный способ мошенничества.

Социальная инженерия – это метод манипуляции людьми, при котором мошенники вынуждают жертву добровольно раскрыть конфиденциальную информацию (пароли, данные карт, коды подтверждения) или совершить опасные действия (перевод денег, установка вредоносного программного обеспечения).

Наиболее распространенные способы мошенничества

1. Финансирование ВСУ и терроризма

Мошенники звонят под видом ФСБ или полиции и запугивают жертв уголовной ответственностью за якобы «финансирование ВСУ» или «поддержку терроризма». Утверждает, что уже возбуждено уголовное дело (возможные используемые в разговоре статьи УК РФ: ст. 205.1. «Содействие террористической деятельности», ст. 275. «Государственная измена» и др.). Начало этой схемы как правило реализовано через мессенджеры.

Далее уговаривают жертву перевести деньги на «безопасный счет» (на самом деле, мошеннику), чтобы избежать ареста или оплатить взятку, чтобы дело закрыли.

Также могут втираться в доверие, говоря, что понимают, что скорей всего Вас использовали «в темную» или без Вашего ведома взломали Ваши счета и предлагают перевести деньги на «безопасный счет», якобы для того, чтобы выявить настоящих преступников или их пособников.

Как защититься:

- **Не переводите деньги** – никаких «безопасных счетов» не существует
- **Не называйте никакие личные данные, не направляйте никакие документы (их копии, фотографии, сканы)** – ФСБ и полиция не запрашивают их по телефону
- **Проверяйте информацию** – позвоните в официальное отделение полиции или банка
- **Игнорируйте угрозы** – если Вас запугивают, положите трубку, не отвечайте на последующие звонки и/или содержащие угрозы сообщения с незнакомых телефонных номеров (часто после того, как жертва кладет трубку, ей начинают последовательно и неоднократно поступать звонки или сообщения с разных телефонных номеров) и немедленно обратитесь в правоохранительные органы
- **Не реагируйте на срочность** – Если Вас торопят, то хотят, чтобы у Вас не было времени подумать и проанализировать ситуацию
- **Проконсультируйтесь с другими людьми** – Позвоните в банк, полицию, друзьям или родственникам. Мошенники будут требовать, чтобы Вы никому не сообщали информацию, якобы ситуация требует секретности, им нужно, чтобы Вы оставались один на один с проблемой.

2. Кража доступа к Госуслугам

Используются схемы для получения кодов доступа. Например, звонят от имени мобильного оператора, просят «продлить договор», о проверке счетчиков ЖКХ, выдаче ключей от домофона и просят сообщить код из SMS, который на самом деле предназначен для входа на Госуслуги. Получив его, мошенники получают контроль над аккаунтом и могут оформлять займы на имя жертвы.

Как защититься:

- **Никогда и никому не сообщайте коды из SMS** – банки и государственные органы их никогда не запрашивают
- **Включите двухфакторную аутентификацию** на Госуслугах и в банковских приложениях

- **Проверяйте ссылки** – официальные сайты имеют HTTPS и правильное написание (например, gosuslugi.ru, а не gosuslugi-verify.com).

3. Кража денег с помощью NFC-модуля смартфона

Новый метод, который позволяет транслировать данные карты при помощи NFC-модуля телефона (электронный компонент смартфона, который обеспечивает работу технологии беспроводной связи ближнего радиуса действия (до ~10 см). Позволяет использовать смартфон в качестве банковской карты, без физического присутствия самой карты). Мошенники звонят гражданам, представляясь сотрудниками банков, и предлагают установить обновленное приложение по предоставленной ссылке. Внешне приложение выглядит как официальное, однако при активации оно запрашивает ПИН-код от карты, что является нарушением политики безопасности финансовых учреждений. Так злоумышленники узнают ПИН-код от карты.

Далее «оператор» банка просит провести «верификацию» и поднести банковскую карту к NFC-модулю смартфона. На деле же фейковое банковское приложение считывает данные с карты и отправляет их на телефон мошенника, далее данные передаются на считыватель банкомата. Как итог – преступник может обналичить средства, не имея доступа к физической карте, а используя передаваемый через устройство сигнал как радиоудлинитель между картой и банкоматом.

Существует и обратная схема, при которой программное обеспечение, установленное у жертвы и мошенника, меняется ролями. Жертве сообщают, что нужно внести средства на «безопасный счет». Она подходит к банкомату, в этот момент мошенник подносит свою карту к своему телефону, информация с карты передается на телефон жертвы. Жертве диктуется ПИН-код и, полагая, что операция проводится с ее картой, она вносит наличные. На самом деле деньги зачисляются на карту злоумышленника.

Как защититься:

- **Не устанавливайте приложения по ссылкам** – скачивайте только из официальных магазинов (Ru-store, App Store, Google Play) или на официальном сайте банка
- **Никогда не вводите ПИН-код карты в приложениях** – банки этого не требуют
- **Проверяйте отправителя SMS** – если пришло подозрительное сообщение «от банка», перезвоните по официальному номеру
- **Установите на свои устройства проверенные антивирусные программы и регулярно обновляйте**.

4. «Ваш родственник попал в беду»

Это одна из старейших схем социальной инженерии, где мошенники играют на любви и страхе человека за близких. Жертвами часто становятся пожилые люди, родители, бабушки и дедушки, но под удар может попасть любой.

В основном реализована в двух вариантах:

Вариант 1: «Это полиция/больница! Ваш [сын/внук/муж] попал в ДТП (арестован, заложник). Нужны деньги на лечение/штраф/выкуп!»

Вариант 2: Сам «родственник» плачет в трубку: «Меня избили, срочно нужны деньги, иначе посадят/убьют!»

Как защититься:

- **Не паникуйте** – сразу перезвоните родственнику на известный вам номер
- **Не верьте в срочные выплаты** – полиция и больницы никогда не требуют переводов
- **Проверяйте информацию** – позвоните в больницу или отделение полиции

- **Предупредите пожилых родственников** – они чаще становятся жертвами таких схем.

5. Получение доступа к личному кабинету/приложению банка

Мошенники связываются с клиентом (обычно под видом службы безопасности банка/Госуслуг) и под различными предлогами (вышло новое приложение или в целях безопасности) уговаривают установить приложение с удаленным доступом к устройству или с записью экрана.

Получив удаленный доступ к смартфону, мошенники могут зайти в банковские приложения и вывести все деньги.

Получив доступ к записи экрана, мошенники будут видеть смс/push-коды, которые всплывают на экране смартфона, и с их помощью могут осуществить вход в приложения банков с другого устройства.

При этому мошенники продолжают удерживать клиента на линии, чтобы он ничего не увидел и не заподозрил.

Как защититься:

- **Никогда не устанавливайте программы, предоставляющие удаленный доступ к Вашему устройству, такие как TeamViewer, AnyDesk и т.д.** по просьбе «службы безопасности». Вообще не устанавливайте приложения (особенно по просьбе третьих лиц по телефону), если не знаете их предназначение и функционал
- **Не разрешайте доступ к экрану** – банки никогда не просят этого
- **Никогда и никому не сообщайте коды из SMS/Push** – даже если звонящий представляется сотрудником банка
- **Никогда не открывайте файлы (фото, видео и т.д.), неожиданно полученные даже от знакомого Вам лица, полученные от неизвестного источника и/или сопровождаемые манящими либо провокативными, но обезличенным обращением (например, «Посмотри, ты ли на этом фото?»)** – данные файлы могут содержать в себе вредоносное программное обеспечение, предназначенное для получения злоумышленниками удаленного доступа к Вашем устройству и установленным на нем банковским приложениям. Помните, что такие файлы могут быть переданы Вам под любым предлогом и даже от Ваших контактов (родственников, друзей, коллег), если их устройство подверглось успешной атаке злоумышленников
- **Никогда не скачивайте и не устанавливаете неожиданно полученное даже от знакомого Вам лица или полученные из непроверенного источника файлы с расширением «АРК» (например, «фото с праздника.АРК»)** – данные файлы могут содержать в себе вредоносное программное обеспечение, предназначенное для получения злоумышленниками удаленного доступа к Вашем устройству и установленным на нем банковским приложениям. Помните, что такие файлы могут быть переданы Вам под любым предлогом и даже от Ваших контактов (родственников, друзей, коллег), если их устройство подверглось успешной атаке злоумышленников
- **Установите на свои устройства проверенные антивирусные программы и регулярно обновляйте их**.

6. Атака через детей

Мошенники активно вовлекают детей и подростков в преступные финансовые схемы, используя их доверчивость, неопытность и доступ к гаджетам.

Мошенники выходят на контакт с детьми через чаты в популярных играх, мессенджеры, телеграм-каналы, социальные сети и под различными предлогами уговаривают детей взять

смартфон родителей и продиктовать смс-коды (для подтверждения переводов или восстановления доступа к банковским приложениям).

Также ребенок может скачать взломанную игру, внутри которой находится вредоносное программное обеспечение, которое крадет логины/пароли от банковских приложений.

Как защититься:

- **Объясните детям простым, понятным и доступным языком**, что никому и никогда нельзя сообщать никакие личные данные, коды из SMS и переводить деньги
- **Научите детей, как и что им необходимо делать и что категорически нельзя делать**, если вдруг с ними на связь выйдут «сотрудники» ФСБ, полиции, Роскомнадзора, банков, им начнут поступать телефонные звонки и/или сообщения о якобы совершении ими, их родственниками, друзьями и знакомыми противоправных действий, о необходимости сообщить о себе и/или третьих лицах любые данные, передать документы, пароли, коды, совершить операции с денежными средствами
- **Обязательно и регулярно проверяйте**, как дети усвоили два предыдущих правила
- **Не давайте детям доступ** к банковским приложениям
- **Установите родительский контроль** и ограничьте скачивание приложений
- **Проверяйте, какие игры/программы установлены** на детских устройствах
- **Установите на свои устройства и устройства детей проверенные антивирусные программы и регулярно обновляйте их**.

7. Удаленная работа

Злоумышленники рассылают в мессенджерах информацию о вакансиях с высоким доходом. Предлагают выполнять легкие задания и получать за каждое деньги. Примеры заданий: ставить лайки продавцам на маркетплейсах или бронировать отели для поднятия их рейтинга.

Мошенники действительно могут сначала заплатить небольшую сумму, добавить Вас в рабочие группы и отправлять там скриншоты «заработков коллег», чтобы убедить Вас в возможности заработать.

Как защититься:

- **Не верьте в легкие деньги** – если платят за лайки и отзывы, это мошенничество
- **Не вкладывайте свои деньги** – настоящая работа не требует предоплаты
- **Проверяйте работодателя** – ищите отзывы, сайт компании, регистрационные данные
- **Не переходите по подозрительным ссылкам** – мошенники могут заразить устройство.

8. Инвестиции

Мошенники создают сайты и каналы в мессенджерах об инвестициях и криптовалюте с обещаниями доходности выше 20%.

С Вами связывается менеджер или аналитик «инвестиционной компании», предлагает пообщаться в видео-мессенджере (например, Skype) и помочь разобраться в инвестициях. На платформах мошенников Вам показывают поддельные графики, на самом деле деньги не поступают на платформу, а сразу обналичиваются злоумышленниками. Они готовы перевести Вам «прибыль от инвестиций», чтобы завоевать Ваше доверие, но это лишь небольшая часть внесенной Вами суммы.

Если Вы захотите вывести все деньги с платформы, у мошенников найдутся отговорки: нужно оплатить страховку или комиссию за вывод, но ее невозможно удержать за счет внесенной Вами суммы, вывод возможен только в определенный день и т.д. Мошенники всегда ищут способы получить от Вас еще больше.

Как защититься:

- **Помните:** чем выше доходность, тем выше риск. **Доходность выше 25% – это скорее всего обман**
- **Не верьте «гарантиям»** – если обещают 100% прибыль, это мошенники
- **Не переводите деньги в «личные кабинеты»** – настоящие брокеры работают через лицензированные платформы
- **Проверяйте лицензии** на сайте Центрального банка Российской Федерации.

Это только несколько из основных схем мошенничества. О них стоит знать, но ориентироваться только на них не стоит. Мошеннические схемы регулярно обновляются, усложняются, эволюционируют. Легенды мошенников обрастают все более правдоподобными доказательствами (от поддельных удостоверений сотрудников служб до использования инструментов имитации голоса и изображения родственников/знакомых).

Мошенники следят за новостями и подстраивают свои схемы под текущие реалии. Как пример выше – схема мошенничества с «финансированием ВСУ».

При общении с третьими лицами, кем бы они не представлялись, не спешите с принятием решений. Если есть хоть малейшие подозрения что что-то не так, просто положите трубку, отключитесь от общения, подумайте. Даже если сомнений нет, то не переводите деньги в момент общения. Срочный перевод не решит возможных проблем.

Не действуйте импульсивно, старайтесь принимать взвешенные решения.

Общие рекомендации по распознаванию мошенничества и его предотвращению

1. Используйте только официальные и проверенные каналы взаимодействия

Знайте, с 01.06.2025 запрещено взаимодействие с гражданами через любые иностранные мессенджеры (WhatsApp, Telegram, Viber и т.д.) всем кредитным организациям, государственным органам, операторам связи.

Официальные каналы взаимодействия при общении с Банком:
Телефоны: 8 (800) 2000-767, 8 (495) 777-77-87
Форма обратной связи на сайте Банка: https://www.finsb.ru/feedback/
Электронная почта: help@finsb.ru.

2. Не передавайте личные данные – пароли, PIN-коды, CVV-коды карт, коды из SMS никому не сообщайте, даже если звонящий представляется сотрудником банка или государственного органа.

3. Проверяйте сайты и приложения
- скачивайте программы только из официальных магазинов (Ru Store, App Store, Google Play);
- перед вводом данных убедитесь, что сайт настоящий (HTTPS, правильное название);
- не открывайте и не скачивайте файлы от неизвестных источников.

4. Включите двухфакторную аутентификацию – это усложнит доступ злоумышленников к Вашим аккаунтам.

5. Минимизируйте утечку личной информации – мошенники используют личные данные для социальной инженерии. Ограничьте использование этих данных в социальных сетях.

6. **Установите запрет на оформление кредитов и микрозаймов через портал Госуслуги** – это поможет предотвратить несанкционированное оформление займов от Вашего имени.

7. **Не действуйте импульсивно. Не проводите финансовые операции по просьбе третьих лиц** – мошенники играют на срочности, страхе, жадности. Чем более срочно или эмоционально звучит просьба, тем выше вероятность обмана. Если Вы чувствуете, что на Вас давят, угрожают, ставят условие сделать покупку, совершить транзакцию, предпринять действия «либо сейчас, либо никогда» – прерывайте общение. Это точно мошенники.

8. **Расскажите близким о мошенничестве** – Пожилые люди, дети и даже взрослые, незнакомые с современными схемами обмана, часто становятся жертвами мошенников. Расскажите им об этом.