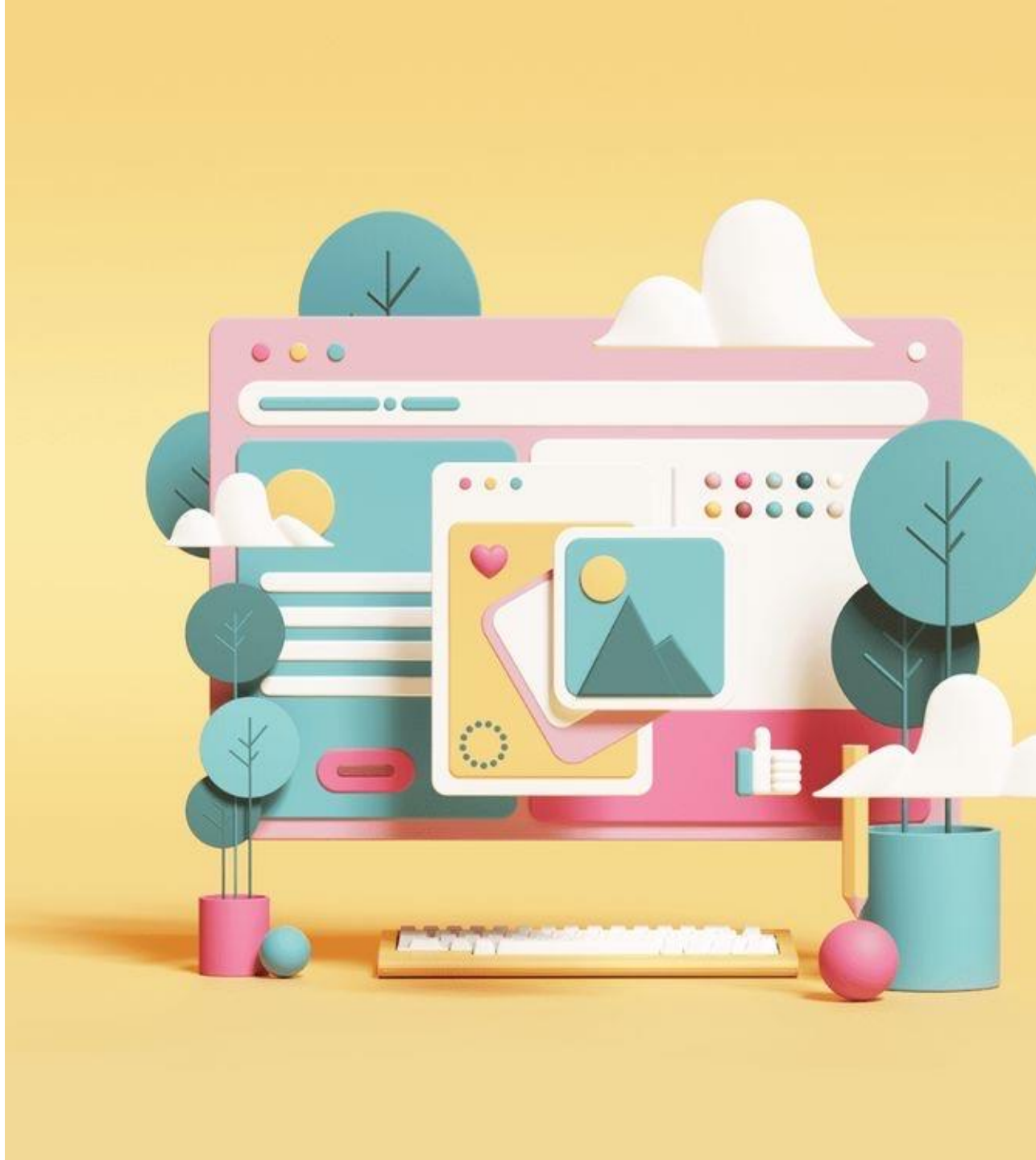
Банк России

Противодействие финансовому мошенничеству
Социальная инженерия



Мошеннические схемы

Люди пожилого возраста

- Сообщение о том, что их денежными средствами кто-то пытается воспользоваться
- Можно запутать разными непонятными терминами

Молодые люди

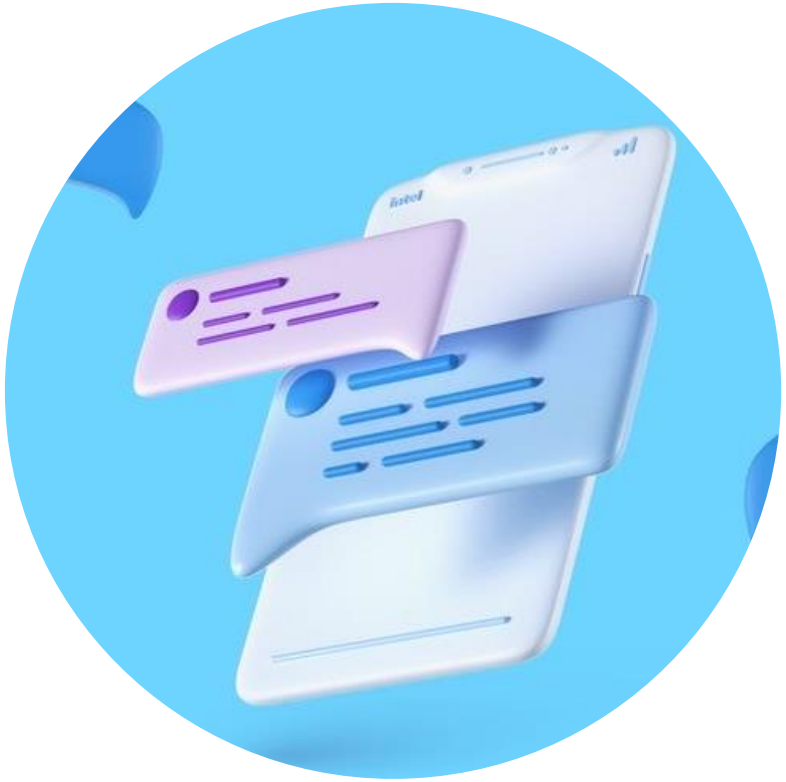
- Возможность заработать, вложив деньги со сверхприбылью
- Предложение сыграть в псевдоконкурсы
- Возможность заработать на новом тренде

Банк России

Социальная инженерия

Социальная инженерия - это методы и приемы психологического манипулирования людьми, чтобы они совершали определенные действия или сообщали конфиденциальную информацию.

Когда мошенники обращаются по имени и отчеству, называют номер карты или другие конфиденциальные данные, кажется, что они представляют знакомую организацию или человека.



Будьте бдительны!

Фишинг

Фишинг - один из видов интернет-мошенничества, который совершается с помощью массовых рассылок СМС, сообщений в чатах и по электронной почте якобы от имени известных интернет-магазинов и сервисов, госорганов, банков и т.д., содержащий ссылку на поддельный сайт, внешне неотличимый от настоящего.

Цель - получение конфиденциальных данных о клиенте.

Банк России

Звонок из банка

Два действующих лица

- псевдосотрудник бюро кредитных историй
- псевдосотрудник банка, правоохранительных органов или Центрального банка

Никаких звонков из банков, из бюро кредитных историй **с информацией об изменении кредитной истории быть не может.**

Банк России

Беспроигрышные лотереи, конкурсы

Мошенники **эксплуатируют тему легкого обогащения:**

- Опрос с заманчивым денежным вознаграждением
- Участие в «беспроигрышных» конкурсах
- Получение социальных выплат
- Возврат налогов

Перейдя по ссылкам на такие сайты, вместо денежных призов **люди получат лишь убытки.**

Банк России

Получение сверхприбыли

Одна из схем – **инвестиции с гарантией сверхприбыли.**

Главное правило инвестирования для легальных финансовых организаций и любых инструментов:
чем больше возможная доходность – тем больше риск.

Гарантировать доходность
на финансовом рынке запрещено!

Банк России

Предложения о работе

Предложения «гарантированной работы» с привлекательными условиями работы: высокой оплатой труда, неполным рабочим днем, легкими задачами — популярный прием мошенников.

Не доверяйте рассылкам с предложением о работе, в которых вас заставляют оплатить какие-либо услуги, товары, зарезервировать вакансию и провести другие платежи.

Банк России

Вам одобрен кредит

Двухступенчатая схема обмана

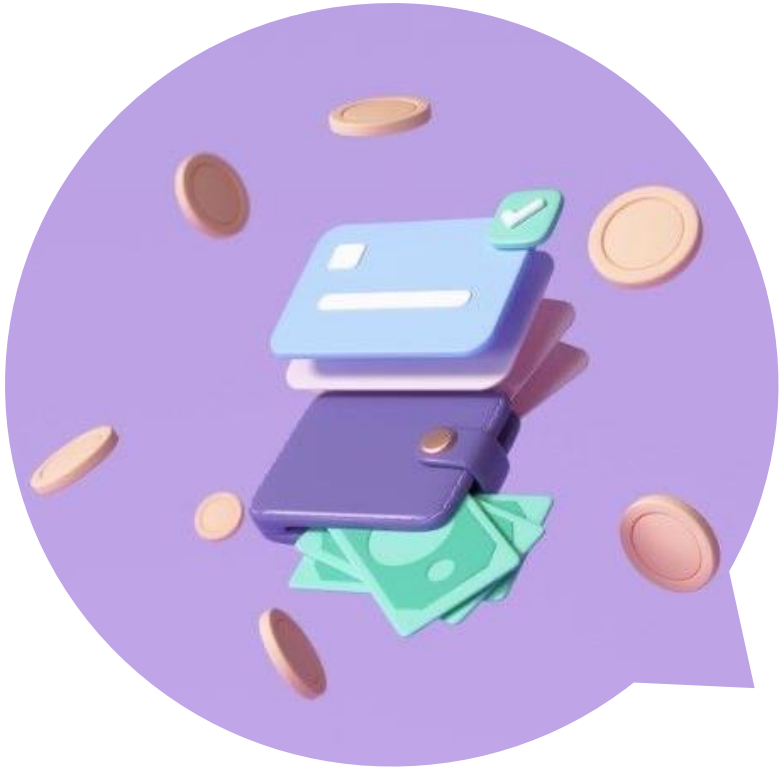
Звонок от имени финансовой организации
с информацией о первоначально одобренном кредите или кредитной карте.

Звонок от якобы службы безопасности банка или полиции, которая **просит оказать помощь** в расследовании и поимке мошенников.

Банк России

Обналичивание денежных средств

Зачастую человек сразу **не понимает, что его вовлекают в преступную схему.**



Если вы понимаете, что деньги точно переведены не вам, не знаете, от кого они – **обратитесь в банк и скажите, что эти деньги не ваши**, вы не знаете отправителя и не понимаете, зачем они были начислены.

Попросите банк **перевести эту сумму обратно** по тем же реквизитам.

Банк России

Схема обмана с размещением QR-кодов

Сканируя QR-код, человек **попадает в чат-бот**, который под предлогом оформления якобы полагающейся выплаты запрашивает у него личные и финансовые сведения, необходимые для хищения денег с карты.

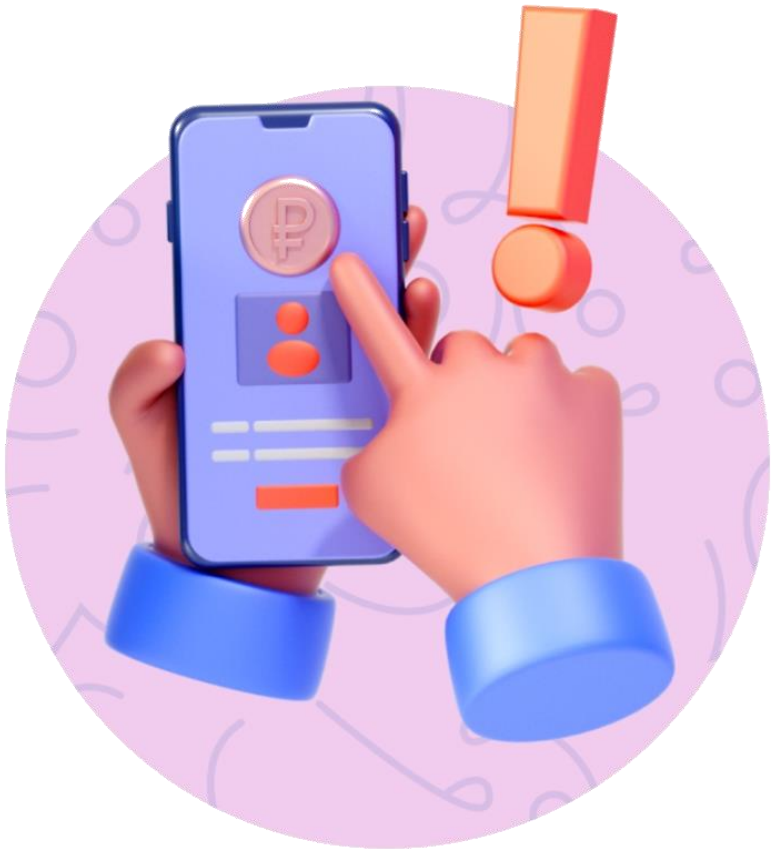
Использование **чат-ботов** у людей **вызывает дополнительное доверие.**

Банк России

Блокировка телефонного номера

Еще одна легенда – **предупреждение о блокировке телефонного номера.**

Попадая на эту уловку, **абонент самостоятельно подключает переадресацию звонков и текстовых сообщений**,
в том числе с СМС-кодами от банка, **на номера мошенников.**



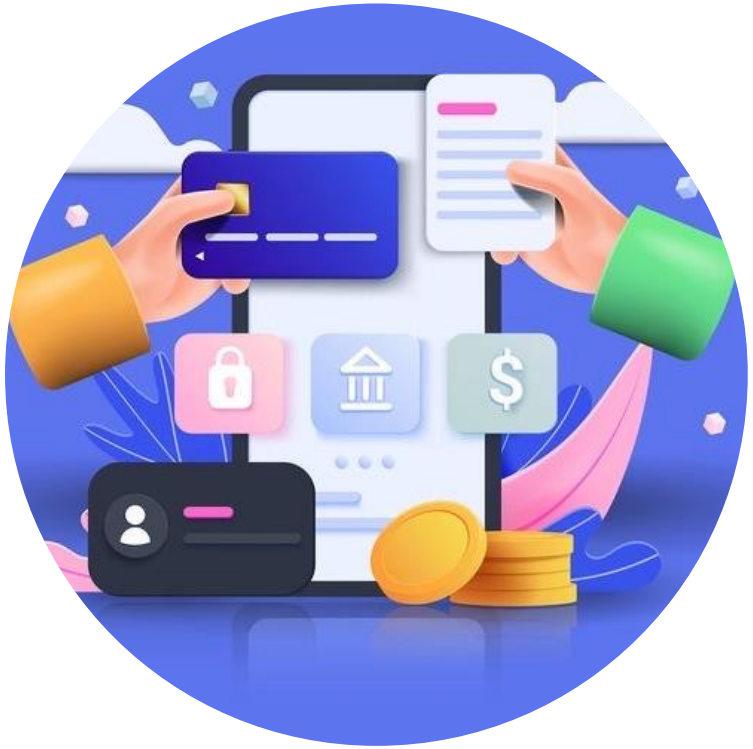
Результат – доступ к дистанционному управлению банковским счетом и **хищение денег.**

Банк России

Сайты с базой данных

Ссылки на сайты, якобы проверяющие утечку банковских сведений.

Как только человек введет на этом сайте свои банковские данные, они оказываются у настоящих мошенников.



Сайтов, на которых можно проверить факт утечки банковских сведений, **не существует!**

Банк России

Базовые правила финансовой безопасности

1. Не сообщайте никому паспортные данные и финансовые сведения.

2. Если с неизвестного номера поступает звонок с требованием быстрых действий с финансами, положите трубку.

3. Помните о том, что Банк России не открывает счета граждан и не работает с ними как клиентами.

4. По возможности установите антивирус на все устройства и обновляйте его.

5. Совершайте покупки в Интернете только на проверенных сайтах.

6. Не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем.

Самое главное правило – никаких переговоров с мошенниками!

Банк России

Если вас обманули мошенники

Шаг 1

Немедленно заблокируйте карту с помощью мобильного приложения, личного кабинета или через контакт-центр банка.

Шаг 2

В течение суток напишите заявление в отделение банка
Также обратитесь с заявлением о хищении денег в любое отделение полиции.

Если вы самостоятельно перевели деньги мошенникам
или предоставили им банковские данные,
то **банк не обязан возвращать** похищенную сумму.

Банк России

Финансовые пирамиды

Это мошеннический проект, который **имитирует выгодные вложения**.

Средства поступают за счет постоянного привлечения новых участников.
Они вносят деньги, затем привлекают новых людей – пирамида растет.

Банк России

Признаки финансовой пирамиды

- Гарантируют высокий доход без всякого риска
- Просят приводить новых клиентов
- Нет подтверждения инвестиций
- На сайте компании нет контактов для связи

Если вы обнаружили **хотя бы один из этих признаков**, стоит серьезно задуматься, кто же на самом деле перед вами.

Банк России

Как не попасть в финансовую пирамиду?

- Найдите финансовую организацию в реестрах Банка России
- Убедитесь, что компании нет в списке сомнительных организаций
- Проверьте данные в госреестре юридических лиц (ЕГРЮЛ)
- Почитайте отзывы в Интернете
- Изучите документы

Банк России

Спасибо за внимание!