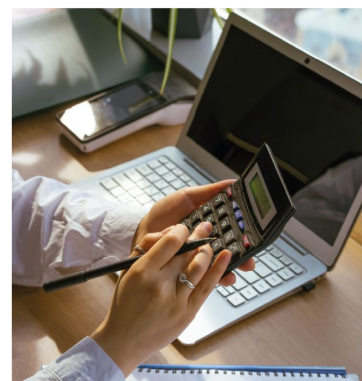


Финансовая безопасность

Как защитить свои деньги
от мошенников?

Наталья Колбасина



Наталья Колбасина

20 лет - опыт успешной работы
в финансовой сфере

Более **60 000** участников
вебинаров и программ

- Руководитель консультационного центра сервиса «Финансовое здоровье»
- Финансовый консультант, бизнес-психолог
- Эксперт на 1 канале и в СМИ
- Автор и ведущая курсов и тренингов по личным финансам для сотрудников крупных компаний и изд. МИФ
- Автор книги «Трачу и приобретаю»



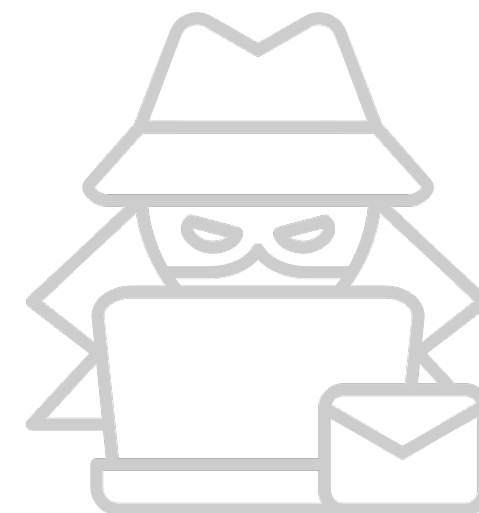
О чем поговорим сегодня

Способы финансового
мошенничества

Как не стать жертвой
мошенников

Правила финансовой
безопасности

Правила психологической
самообороны



15 800 000 000

1 400 000 000 (8,7%)

Почему?

Одна из возможных причин по мнению ЦБ РФ:
более адресные и подготовленные **атаки телефонных мошенников с использованием социальной инженерии.**

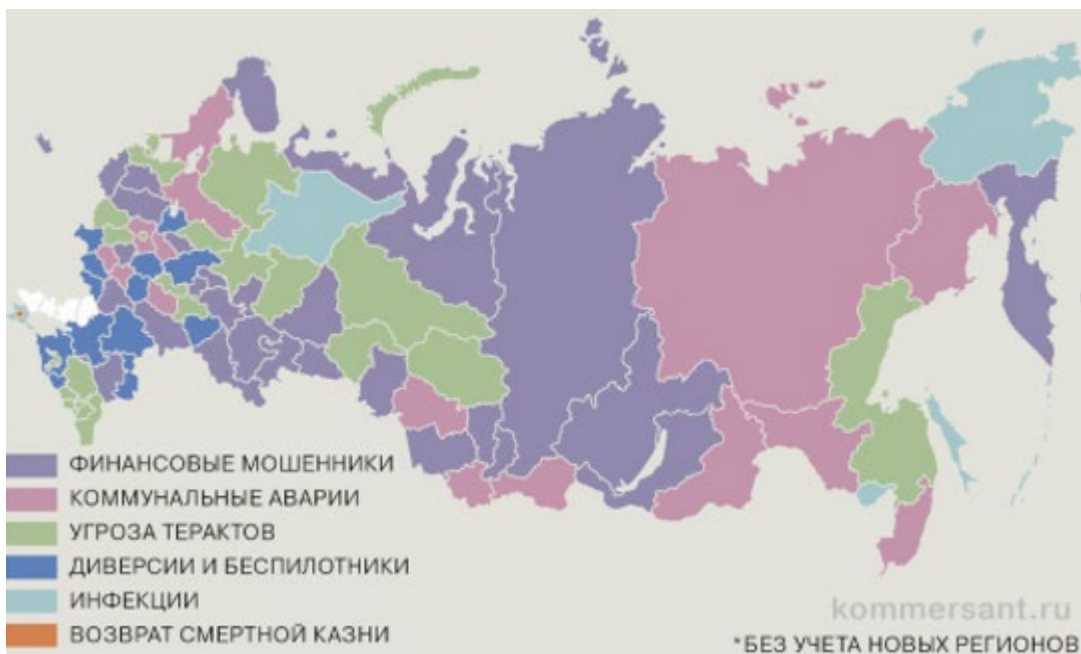
Социальная инженерия - психологическое воздействие мошенником на человека с целью получения конфиденциальной информации или доступа к ней для хищения денег, угона аккаунта и т.п.

Мошенники используют особенности человеческой природы – страх, любопытство, уважение к властям, желание помочь другу.



Страхи россиян

В I кв. 2024 г. боязнь финансового мошенничества вошла в топ-3 страхов в 70 регионах*



* Исследование «Национального индекса тревожностей», КРОС

Тревожность



Насмотренность

Чем больше сразу учишься, тем меньше после мучишься.

Льюис Кэрролл

Способы мошенничества

Фишинг

Интернет-мошенничество с помощью электронных писем, содержащих вредоносные ссылки или вложения.

Вишинг

«Голосовой фишинг». Мошенники по телефону выманивают у жертвы конфиденциальную информацию и заставляют совершить действия со своими счетами, имуществом, деньгами.

Финансовые пирамиды

Мошенническая организация, выплачивающая инвесторам доход за счет денежных средств новых участников проекта.

Тренды вишинга

- Звонки **сотрудников госорганов**: МВД, прокуратуры, Центробанка, МФЦ.
- Телефонное мошенничество **FakeBoss**.
- Звонки представителей **соцслужб**.
- **Лжеброкеры**.
- **Лжеюристы**, предлагающие вернуть деньги, украденные лжеброкерами и брокерам.
- **Аудио и видео дипфейки**.
- Звонки **операторов мобильной связи** для продления сим-карты.
- Рассылка **push-уведомлений** для подтверждения паспортных данных по ссылке, ведущей на сайт якобы оператора, а затем на портал Госуслуг.

Главная особенность - мошенники комбинируют схемы, постоянно расширяют свой арсенал. Используют одновременно методы социальной инженерии и фишинга.

Аудио и видео-дипфейки

Голосовые дипфейки

Мошенники, используя ИИ, подделывают голос человека.

А затем рассылают голосовое сообщение его подчиненным, родственникам, друзьям, подписчикам.

Нейросети могут клонировать голос любого человека и даже добавлять эмоции!

Как защититься:

Позвонить начальнику, другу, родственнику напрямую.

Видео дипфейки

Создание с помощью ИИ поддельного видео с изображением человека.

Как распознать:

- неровное движение;
- перемены освещения в соседних кадрах;
- различия в оттенках кожи;
- человек на видео моргает как-то странно или не моргает вообще;
- плохая синхронизация движения губ с речью;
- Замедленная мимика, безэмоциональность
- Любые изменения (пиксели, цвета) в изображении.

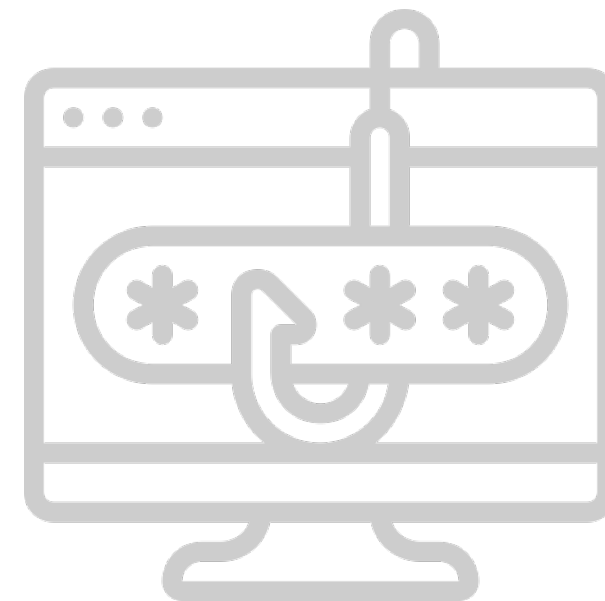
Тренды фишинга

Более 50% россиян столкнулись с фишингом в 2023 году.

В России выявили **212 тыс.** мошеннических сайтов (рост на 48 % по сравнению с 2022 г.)

Трендом фишеров стала охота на аккаунты россиян в мессенджерах.

По итогам 2023 года **Telegram** стал главной площадкой для фишинговых атак и других способов мошенничества в России.



Популярные фишинговые приманки

- Письма о **получении льгот, компенсаций, субсидий** от лица госорганов.
- Выгодные предложения из **игровой сферы** для любителей компьютерных игр.
- **Имитация** популярных **криптовалютных ресурсов** с предложением подключить криптокошелек.
- Массовая рассылка писем от имени **«настоящего» интернет-магазина** с выгодным предложением.
- Письма с **QR-кодами**, ведущими на мошеннические ресурсы.
- Распространение в личных и групповых чатах в соцсетях **ссылок на голосование** за участников конкурсов.
- **Фейковые розыгрыши** призов и лотереи.
- Предложение **банковских услуг** – льготные кредиты, выгодные вклады и т.п.
- Использование ИИ - **«умных чатботов»**, выдающих себя за консультантов по заработку в сети.
- Предложение восстановить **кредитную историю**.
- Предложение **легкого заработка**.
- **Письма «счастья»** о получении крупного выигрыша, наследства.
- Письма от **службы техподдержки банка** - перейти по ссылке и внести изменения в личном кабинете.
- Письма **об отключении или блокировке учетной записи** или ведении в ней подозрительных действий.
- Спам с **вымогательством** за нарушение закона.

Финансовые пирамиды

В 2023 году Банк России выявил **2 944 пирамиды**
(рост на 46% к 2022 г.)

- 98% пирамид - работали в сети интернет.
- 50% - принимали взносы в криптовалюте.

В основном это небольшие псевдоинвестиционные проекты, действующие в интернете. Продвигаются через соцсети и мессенджер Телеграм, рекламу лайфстайл-блогеров с большой аудиторией.

Принимают деньги через иностранные платежные сервисы и криптовалюты.

[Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке](#), сайт ЦБ РФ



Как не стать жертвой мошенников

Знаешь, одна из самых серьезных потерь в битве – это потеря головы!

Льюис Кэрролл



Как не стать жертвой мошенников

Финансовая грамотность



Знание, навыки для
соблюдения правил
финансовой безопасности
в интернете, при
пользовании банковской
картой

Эмоциональная грамотность



Умение распознать
манипуляции и
психологическое
давление и защититься от
финансового внушения

Финансовая грамотность



Цифровой след

Цифровой след — это информация, которую человек оставляет о себе и своих действиях при использовании интернета (посты в соц. сетях, история поиска и просмотров на YouTube, логины и пароли, сохранённые в браузере).

2 вида:


Активный – сами оставляем информацию о себе в сети

Пассивный – появляется без нашего ведома. О нас собирают информацию через рекламные трекеры, файлы Cookies и отпечатки пальцев.

Киберпреступники могут использовать ваш цифровой след в целях фишинга, для доступа к учетной записи или для создания ложных профилей на основе ваших данных.

Как замести цифровой след: [статья Т-Ж,
https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint](https://www.kaspersky.ru/resource-center/definitions/what-is-a-digital-footprint)

Правила кибергигиены

- Никому и никогда не сообщайте ваши персональные данные: трехзначный код с обратной стороны карты или СМС-код.
- Не переходите по ссылкам из подозрительных писем.
- При любом тревожном звонке самостоятельно звоните в банк по номеру телефона, указанному на обратной стороне карты или на сайте.
- Для оплаты онлайн-покупок заведите отдельную виртуальную карту и установите лимиты для совершения покупок.
- Пользуйтесь двухфакторной аутентификацией при входе в интернет-банк (логин-пароль + код в смс).
- Берегите свои персональные данные.
- Придумывайте сложные пароли и регулярно их обновляйте. Используйте разные пароли для захода на разные интернет-ресурсы.
- Совершайте покупки в интернете только на проверенных сайтах. Используйте защищенные сайты, адреса которых начинаются с `https://`, а в окне браузера есть значок . Проверяйте дату создания сайта.
- Не заходите в мобильный банк с общественного Wi-Fi.
- Используйте лицензионные антивирусные программы на всех устройствах и регулярно их обновляйте.
- Регулярно проверяйте кредитную историю.

Полезные ссылки



ЦБ РФ, [Список компаний с выявленными признаками нелегальной деятельности на финансовом рынке](#)



[Как защититься от мошенников](#)
бесплатный курс от Т-Ж



[Пирамидометр Т—Ж](#)
для проверки компаний



МОШЕЛОВКА.РФ



Вместе Против Мошенников



Финансовая
культура

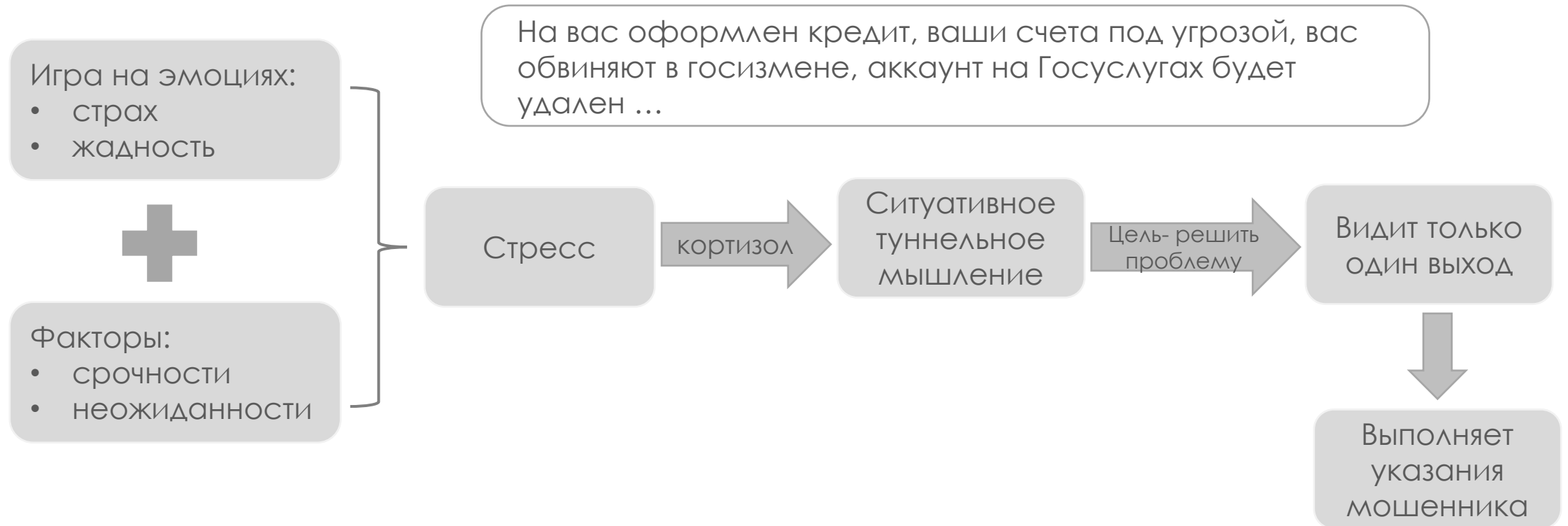
Мошенничество



Эмоциональная грамотность



Эмоции – главные враги для ваших денег



Как защититься?

Не вижу – не верю – проверю



Развивайте здоровую
подозрительность, учитесь
говорить «нет»

Стоп панике!



- Задайте неожиданный вопрос
- Выпить воды
- Техники Mindfulness

Включите тревожную кнопку

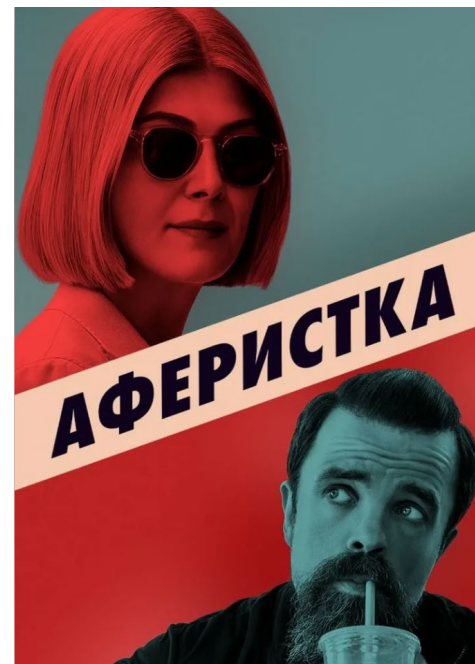
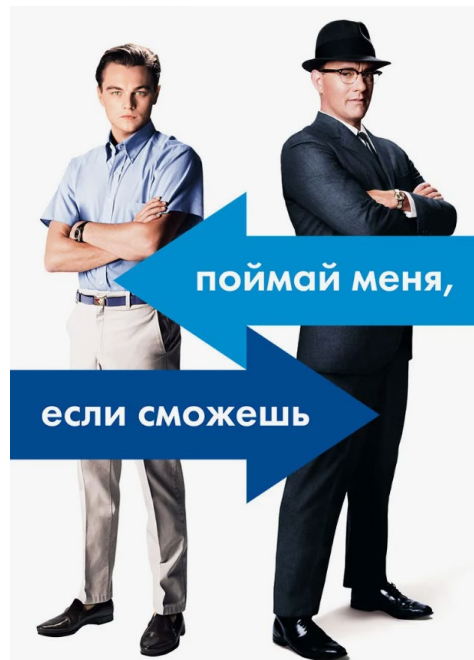


Пробудите внутреннего Ш.
Холмса, Штирлица, Пуаро, мисс
Марпл и положите трубку



Кстати, так советует нам делать ЦБ РФ в своем ролике
[«Пробудите внутреннего Штирлица»](#)

Что посмотреть



Выводы

Не доверяйте и всегда
проверяйте!

Развивайте насмотренность и
критическое мышление

Соблюдайте правила
финансовой безопасности

Повышайте эмоциональную
грамотность

Развивайте привычку– всегда
включать «внутреннюю»
тревожную кнопку!

Делитесь информацией с коллегами,
близкими, пожилыми родственниками

Полезные материалы

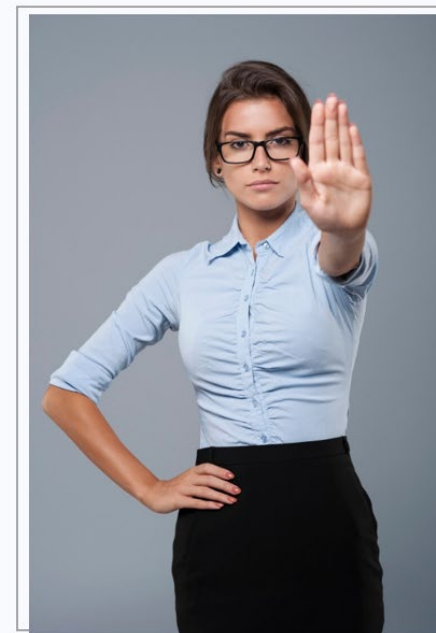
Забрать подробный [гайд](#)



осторожно, мошенники

ФИНАНСОВАЯ БЕЗОПАСНОСТЬ

➔ как защитить свои деньги от мошенников



Автор гайда:
Наталья Колбасина

[@kolbasinafinance](#)



Наталья Колбасина

ФИНАНСОВЫЙ КОНСУЛЬТАНТ

<https://t.me/kolbasinafinance>

