

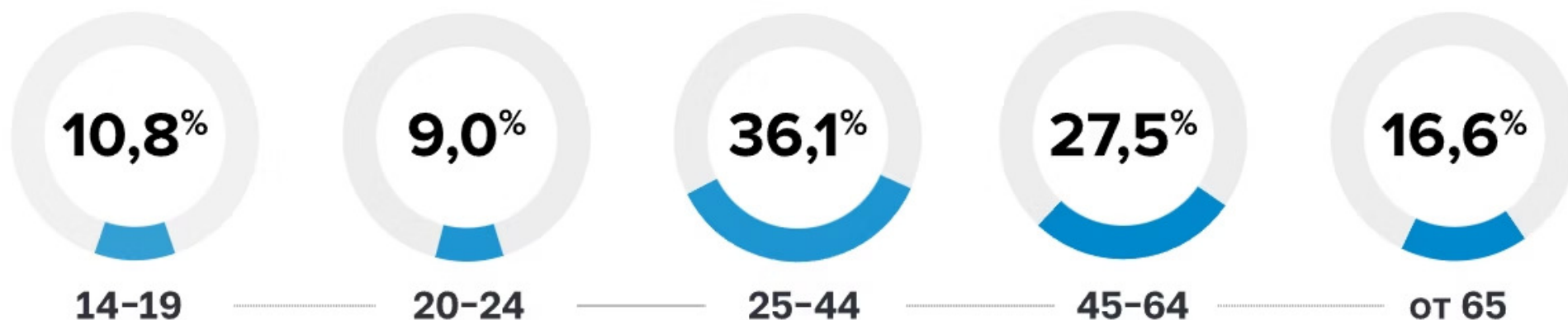


Поведенческие паттерны, которые мешают нам жить и помогают мошенникам

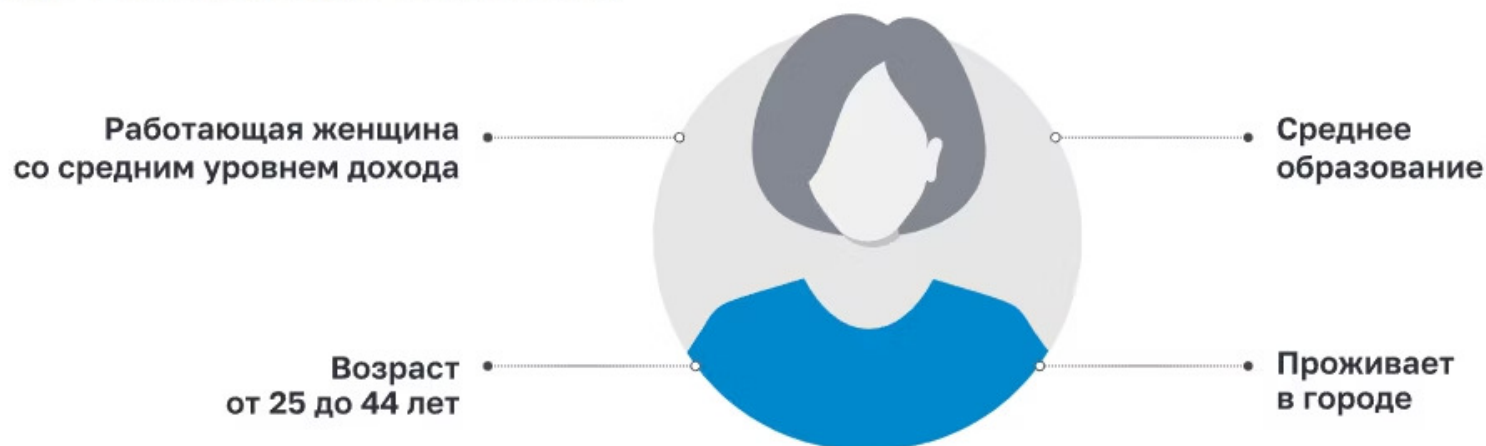
Как психология делает нас уязвимыми перед финансовым
мошенничеством

Чашникова Кристина, независимый эксперт по финансовой
грамотности

Немного статистики по данным ЦБ



В 2024 году жертвами мошенников чаще всего становились работающие женщины со средним уровнем дохода и средним образованием, которые проживают в городе и имеют постоянную занятость.





Что видят в нас мошенники?

Невозможность получения дополнительного заработка, завышенные финансовые ожидания, стремление выглядеть финансово обеспеченным — далеко не исчерпывающий перечень факторов, определяющих экономическое мышление жертвы мошенника.

Грамотность или неграмотность финансовых операций пронизаны психологией, поскольку они связаны с личностью носителя этих действий: индивидуально-психологическими особенностями, социальными установками и стереотипами поведения.

Погхог Т. Bashir

Исследование в Пакистане показало: люди делают вклады в различные институты для получения прибыли, но абсолютно не понимают, как работают финансовые рынки.

Зачем?

1. Хотят "быть в тренде";
2. Хотят быстро заработать;
3. Гордятся тем, что "зашли на рынок"



Что видит мошенник?

Самое первое - отсутствие понимания, как работает рынок, то есть можно сказать красивыми словами всё, что угодно и жертва не поймет.

Второе - желание быстро заработать, чем мошенник точно воспользуется, предлагая "выгодную" сделку на условиях лучше рынка, сокращая срок получения дохода.

Третье - желание быть в тренде. В гордыне жертвы мошенник найдет чем зацепить человека, который хочет соответствовать визуальному статусу "инвестора". Зацепит тем, что все уже разобрались, все инвестируют, а ты один остался позади планеты всей. Все уже заработали состояния, а ты всё ещё думаешь, соглашаться или нет?

Психологические факторы, влияющие на финансовое поведение

Чувство безысходности

Влияет на принятие финансовых решений

Религиозность

Определяет отношение к деньгам

Зависимость от общественного мнения

Склонность к рискам

Предиктор финансового поведения

Отсутствие навыка получения отложенного удовольствия

Определяет склонность к принятию импульсивных решений

Четыре составляющие мышления финансово грамотного человека (по мнению J. Gathergood)

01

Оптимизм

Оптимистичные люди финансово успешны и принимают более взвешенные решения

02

Взвешенность решений

Не потенцирует безрассудные финансовые поступки и необдуманные траты

03

Целеполагание

Ориентация на достижения существенно повышает финансовую грамотность

04

Локус контроля

Финансово успешным людям свойственен интернальный локус контроля (убеждение человека в том, что он сам контролирует свою жизнь и свои результаты, а успех или неудача зависят от его собственных усилий, навыков и решений, а не от внешних обстоятельств)

📌 **J. Gathergood акцентирует:** самоконтроль является ключевым предиктором финансово грамотного поведения



Психологический портрет человека-жертвы



Чувство беспокойства

Постоянная тревога о финансовом будущем

Негативная оценка

Пессимистичный взгляд на происходящее вокруг

Социальная тревожность

Неуверенность в социальных взаимодействиях

Неудовлетворенность жизнью

Общее недовольство жизнедеятельностью



Молодежь Южной Африки: тревожные корреляции

Исследование С. Mudzingiri, J.W.M. Mwamba и J.N. Keyser демонстрирует опасные связи между низкой финансовой грамотностью и поведенческими паттернами:



Излишняя самоуверенность

Переоценка своих финансовых способностей



Склонность к рискам

Готовность к необдуманным финансовым действиям



Нетерпеливость

Желание быстрых результатов без планирования

Пример для самоанализа: импульсивный онлайн-шоппинг

Факторы риска

Низкий уровень финансовой грамотности выступает как личностный фактор риска проблематичного онлайн-шоппинга.

Проанализируйте, как часто вы заходите на маркетплейсы, сколько времени прошло с момента возникновения желания что-либо купить до момента непосредственной покупки.

Импульсивные покупки в интернете приучают нас к получению "быстрого" удовольствия. Как правило, необдуманного.



Проблема современных программ финансовой грамотности

К сожалению, многие организации, которые занимаются финансовой грамотностью, ориентированы на преимущественно непсихологические методы повышения финансовой грамотности населения.

Что делают сейчас

- Повышают осведомленность о банковских продуктах
- Объясняют финансовые инструменты
- Дают много терминов, формул, усиливают навыки

Что нужно добавить

- Психологическая диагностика
- Тренинги по самоконтролю
- Консультирование по поведенческим паттернам - осознание проблемы - это 50% успеха в её решении

Психология — ключ к защите от мошенников



Психологические аспекты

Должны занять центральное место в программах финансовой грамотности



Профессии риска

Особое внимание на финансовое поведение уязвимых групп населения



Комплексный подход

Сочетание технических знаний и психологической устойчивости



Понимание собственных поведенческих паттернов — первый шаг к защите от манипуляций мошенников

Факторы, усиливающие риски финансового мошенничества

- Усложнение FinTech отрасли и увеличение количества зон уязвимостей финансовых систем всех уровней;
- Высокая волатильность на финансовых рынках, нестабильность мировой экономики и снижение уровня покупательской способности у жителей ряда стран;
- Сверхвысокие доходы участников финансовых афер при весьма умеренном наказании в большинстве стран мира;
- Несоответствие поведенческих стереотипов участников финансово-денежных отношений новому уровню рисков.

Признаки, указывающие на риски финансового мошенничества

- вознаграждение существенно превышает деловую практику по данному типу сделок и несоразмерно объему инвестиций или затратам труда;
- использование технологии «социальной инженерии» и манипулирование такими чувствами как жадность, зависть, желание быстро разбогатеть;
- предложение решить все финансовые проблемы в короткий срок;
- необходимость первоначальных выплат;
- анонимность контрагента;
- необходимость мгновенного принятия сложного финансового решения;
- несоответствие складывающейся ситуации стандартной схеме;
- наличие указания на эксклюзивный, кастомизированный характер предложения.

Социальная инженерия. Психологические приемы повышения уровня доверия

- мошенники уже обладают каким-то объемом информации про нас – чаще всего это номер телефона, ФИО, город проживания; реже данные карты, банка эмитента, остатка на карте.
- подмена телефонного номера в соответствии с целевым звонком стиль общения – сугубо деловой, имитирующий стиль общения в соответствующих организациях
- фон, за голосом говорящего, слышно присутствие большого количества говорящих людей, имитирующее колл-центр
- зачастую телефонный разговор начинает робот со стандартными фразами и только потом подключается живой человек
- использование в разговоре специальных финансовых терминов
- включение в разговор нескольких людей с разными ролевыми позициями

Поведенческие стереотипы потерпевших от финансовых мошенничеств (I)

- нацеленность на высокий гарантированный доход;
- неадекватно высокий уровень доверия к незнакомым и малознакомым контрагентам;
- отсутствие критического взгляда на фактическое состояние ситуации;
- нарушение регламента пользования финансовыми инструментами;
- невнимательность при осуществлении финансовых транзакций;
- нежелание погружаться в детали сделки или читать условия договора в полном объеме.

Поведенческие стереотипы потерпевших от финансовых мошенничеств (II)

- отказ от советов и консультаций профессиональных юристов и экономистов при оценке и заключении сделки;
- готовность к принятию быстрых необдуманных финансовых решений;
- игнорирование предупреждений и дисклеймеров контролирующих и правоохранительных органов;
- технологическая отсталость в условиях современных финансовых взаимодействий;
- высокая готовность к риску, зачастую на грани «русской рулетки».



Принципы ответственного поведения на финансовых рынка

Используйте принцип нулевого доверия:

- не ищите на финансовых рынках "бесплатный сыр"
- не поддавайтесь на уловку "только для вас"
- не торопитесь при принятии финансовых решений
обращайтесь за консультациями и советами в
лицензированные финансовые учреждения, к
друзьям, знакомым, родственникам
- не инвестируйте в высокорисковые активы,
особенно в криптовалютный рынок и рынок
форекс

Поиграем? Безопасно ли... ставьте +, если считаете безопасным, -, если нет

Оплата биометрией

Банки позволяют получать услуги дистанционно, без предъявления паспорта, а магазины и рестораны внедряют оплату по распознаванию лица — достаточно просто посмотреть на камеру. Однако для этого требуется предоставить свои биометрические данные. Насколько надёжна такая практика и какие риски она несёт?



Ответ: да, безопасно

Кибермошенникам крайне сложно подделать биометрию: для идентификации ЕБС требует живое видео с произнесением случайных чисел — система анализирует мимику, движение глаз, глубину и другие параметры. Даже продвинутые атаки (грим, дипфейки, анимация лица и синтез речи) выявляются ИИ благодаря несоответствию опорных точек и отсутствию «живых» признаков.

Что касается утечки данных — биометрия хранится в зашифрованном виде на защищённых системах с высочайшими стандартами безопасности. Расшифровать и использовать её злоумышленники не могут. Подтверждённых случаев утечки биометрических данных в ЕБС — нет.

Можно ли произносить "да", "согласен" и другие подтверждающие фразы?

После появления возможности совершать финансовые операции и получать госуслуги при помощи биометрии данной технологией заинтересовались и мошенники. Они пытаются раздобыть фотографии и записи голоса человека. Еще в 2021 г. появились публикации о подозрительных звонках, когда человека просили громко и чётко произнести фразы «я согласен», «я подтверждаю», «да», «нет». - данные взяты с сайта Сбербанка

Можно!

По той же причине:)

Говорить «да» по телефону совершенно безопасно. Дело в том, что ни на одном крупном интернет-ресурсе не предусмотрено входа в учетную запись по слову «да». Для авторизации чаще всего нужно указать логин и пароль либо ввести одноразовый код из СМС.

Также не стоит бояться, что запись голоса используют в банке, где предусмотрен вход по биометрическим данным. Когда пользователь сдает биометрию, то его просят сказать вслух несколько цифровых комбинаций. Компьютерная программа с помощью специальных технологий разбирает звуки на мельчайшие детали. Учитывается тембр, интонация, громкость, другие особенности речи. Даже самые современные нейросети не смогут воспроизвести голос человека со 100%-ной точностью: система банка сразу распознает дипфейк.

Если вам перевели деньги "случайно" и просят вернуть по номеру карты. Вы их возвращаете по указанному номеру?

На телефон приходит уведомление от банка с информацией о зачислении некой суммы на счет. Следом звонит неизвестный и говорит, что отправил перевод не туда, куда планировал. Он просит вернуть финансы.



Нет, небезопасно

Проверьте реквизиты получателя, куда просят вернуть деньги. Зачастую мошенники просят перевести деньги по номеру карты.

На первый взгляд, человек ничего не теряет — просто возвращает «чужие» деньги. На деле он становится дроппером: его счёт используют для «отмывки» похищенных средств и маскировки следов преступников. Чем больше таких посредников, тем труднее выйти на настоящих организаторов. В итоге невинному придётся доказывать полиции, что он не причастен к мошеннической схеме.

Перед звонком преступники тщательно прорабатывают сценарий, применяя приёмы социальной инженерии и манипуляции, чтобы вызвать у жертвы сильные эмоции — страх, азарт, ложную надежду. Как только эмоциональный крючок сработал, остаётся лишь направить человека по нужному пути: перевести деньги, снять наличные, передать курьеру — а под давлением он может даже оформить кредит или продать имущество, лишь бы «спасти ситуацию» по инструкции мошенников.

Выводы

Вывод:

Мошенники успешно обманывают людей не за счёт технической сложности, а благодаря глубокому пониманию поведенческих паттернов: они целенаправленно запускают эмоциональные триггеры — страх потери, жадность, срочность, доверие к «официальным» источникам. Когда человек действует в состоянии стресса, спешки или эмоционального возбуждения, рациональное мышление отключается, и он легко следует инструкциям преступников, игнорируя красные флаги.

Ключевые уязвимости:

- **Автоматизм решений** — привычка быстро реагировать на звонки/сообщения без проверки;
- **Склонность к доверию** — особенно к тем, кто представляется сотрудником банка, правоохранителей или близким человеком;
- **Страх перед последствиями** — «если не сделаю сейчас — всё пропало»;
- **Социальное давление** — стыд, вина, желание «исправить ошибку».

Защита начинается с осознанности: *остановиться, выйти из эмоций, проверить информацию независимо* — даже одна пауза может остановить преступление.

Список литературы

Bashir T., Arshad A., Nazir A., Afzal N. Financial literacy and influence of psychosocial factors // European Scientific Journal. 2013. Vol. 9. N° 28. P. 384-404

Gathergood J. Self-control, financial literacy and consumer over-indebtedness // Journal of Economic Psychology. 2012. Vol. 33. Iss. 3. P. 590-602.

Mudzingiri C., Mwamba J.W.M., Keyser J.N. Financial behavior, confidence, risk preferences and financial literacy of university students // Cogent Economics & Finance. 2018. Vol. 6. N° 1.

Официальные сайты Сбербанка, ВТБ, РБК, ЦБ РФ