Исследование Тинькофф: как происходит мошенничество в российской банковской сфере

**Москва, Россия — 10 марта 2020 г.** Тинькофф провел масштабное исследование мошенничества в российской банковской сфере. Аналитики компании выявили самые распространенные методы хищений средств у клиентов российских банков\*, подсчитали средние суммы потерь для различных преступных сценариев, составили Fraud Index (индекс подверженности мошенничеству) для разных социальных групп, а также описали типичные схемы обмана.

**Основные выводы:**

* *На социальную инженерию приходится 70% от всех случаев успешного мошенничества. 41% - это случаи, когда пострадавшие сам переводит деньги злоумышленникам. В**29% случаев клиенты предоставляют преступникам данные карты и коды из смс;*
* *За два года доля социальной инженерии в общей структуре фрода выросла в 2 раза;*
* *Средняя сумма для всех попыток мошенничества - около 14 000 руб., за год эта цифра сократилась на 13%. При этом средний чек успешного фрода составляет 9300 рублей.*
* *Женщины становятся жертвами мошенников реже, чем мужчины;*
* *Люди, состоящие в браке, попадаются на уловки мошенников почти вдвое реже, чем неженатые;*
* *Больше всего подвержены мошенничеству молодые люди до 33 лет и старше 68 лет;*
* *Клиенты банков с ученой степенью чаще всего самостоятельно переводят деньги преступникам - в 2,3 раза чаще чем клиенты с начальным и средним образованием*
* *Основные каналы выхода мошенников на клиентов - телефон и социальные сети*
* *Технологии машинного обучения помогли сократить средний чек при утере/краже карты за два года почти в два раза - до 9 800 руб.*
* *Типичные и нетипичные схемы мошенничества и базовые правила безопасности описаны в конце исследования.*

Доля мошенничества с использованием социальной инженерии в 2019 году составила около 70% от всех случаев фрода с реальными потерями клиентов. Под социальной инженерией в данном случае подразумеваются сценарии, когда клиент осуществляет перевод мошенникам самостоятельно или предоставляет им платежные данные по своей воле.



За два года доля социальной инженерии в общей структуре по всем видам мошенничества увеличилась практически в 2 раза - на начало 2018 года она составляла 36%.

По данным на начало 2020 года 41% от всех случаев успешного мошенничества приходятся на схемы социальной инженерии, при которых клиенты самостоятельно переводят деньги злоумышленникам. За 2019 год доля подобных сценариев в общей структуре фрода выросла в два раза, за 2018-2019 гг - в четыре раза.

В 29% от всех успешных случаев фрода клиенты банков сами раскрывают мошенникам данные банковской карты и смс-коды, с помощью которых далее злоумышленники сами списывают деньги.

12% мошеннических случаев приходится на friendly fraud, когда друзья или родственники клиентов обманным путем получают доступ к данным их карт или смартфонам. Еще 11% — это операции без присутствия карты, которые проводятся в торговых точках, не требующих смс-коды для платежей.

Долю в 7% занимают случаи мошенничества с украденными или утерянными картами. Скимминг (использование специальных технических устройств для считывания данных карты клиента) — практически исчез с рынка из-за высокой стоимости и сложности для мошенников. Его доля в общей структуре составляет на сегодняшний день около 1%.



**Социальный портрет**

*Пол*

43% от всех случаев успешного фрода приходится на женщин (средний чек 12 700 рублей), 57% - на мужчин (средний чек 11 600 рублей).



Мужчины также переводят деньги чаще по собственной воле чем женщины (59% vs 41%). При этом женщины чаще самостоятельно предоставляют данные мошенникам в сценариях социальной инженерии (смс-коды и данные карты) - 58% случаев и 42% у мужчин.

*Возраст*

Чаще всего жертвами мошенничества становятся клиенты банков в возрастной категории 28-37 лет - на них приходится 39% от всех успешных случаев фрода со средним чеком 10 тысяч рублей.



*Fraud Index - это показатель, характеризующий подверженность социальной группы клиентов мошенничеству. Для его расчета аналитики выбрали категорию с наименьшими показателями случаев мошенничества на общее количество клиентов и присвоили ей единицу. Остальные категории относятся к ней в прямой пропорции. Например, в категории с показателем 1,30 клиенты становятся жертвами мошенников на 30% чаще, чем группа 1,0.*

Самая уязвимая группа клиентов – от 18 до 22 лет. Так, например, они становятся жертвами злоумышленников на 60% чаще, чем клиенты в группе от 48 до 62 лет. Люди от 68 до 72 лет — на 40% чаще, от 23 до 27 лет — на 35%.

****

Молодые люди гораздо чаще, чем зрелые и пожилые клиенты переводят деньги мошенникам добровольно. Например - за покупку несуществующего товара в интернете или под предлогом “выгодной” инвестиции. Так, например, Fraud Index в категории 18-22 лет составляет 4,37.

Возрастные клиенты, наоборот, чаще предоставляют злоумышленникам смс-коды и данные карт: пожилых клиентов легче обмануть, чем людей среднего возраста. Чем выше возраст, тем выше Fraud Index для этого сценария социальной инженерии.

*Образование*

Клиенты с высшим образованием становятся жертвой мошенников также часто, как с начальным и средним образованием. Клиенты с учеными степенями становятся жертвами преступников в 1,5 раза чаще, чем клиенты с высшим, начальным или средним образованием. Люди с двумя и более высшими образованиями — на 30% чаще.



При этом люди с начальным и средним образованием чаще всего разглашают злоумышленникам данные смс-кодов и карт. Но клиенты банков с ученой степенью чаще всего самостоятельно переводят деньги преступникам - например, в 2,3 раза чаще чем, клиенты с начальным и средним образованием.



*Семейное положение*

Как показало исследование, люди, состоящие в браке, меньше подвержены мошенничеству. Холостые и незамужние, а также разведенные и овдовевшие клиенты становятся жертвами преступников чаще на 40-50%.



У людей, состоящих в официальном браке, как правило, общий семейный бюджет - в отличие от многих пар, живущих в гражданском браке. Они чаще советуются по финансовым вопросам с супругами и и те могут повлиять на их решение.

**~~~~**

**Каналы взаимодействия клиентов и мошенников**

Для разных сценариев социальной инженерии характерны собственные схемы выхода мошенников на клиентов российских банков.

Так, например, в сценариях, когда клиенты разглашают смс-коды и данные карт, в 83% случаев злоумышленники звонят своим жертвам по телефону, а в 17% случаев находят их в мессенджерах, завлекают через объявления, по e-mail и т.д. Средний чек для мошенничеств по телефонному каналу для таких сценариев составляет 34 000 руб., для других каналов - 16 000 руб.

В схемах, связанных с добровольным переводом средств, структура другая: в 32% случаев клиенты российских банков и мошенники находят друг друга в социальных сетях - например, продают или покупают товары в интернете. В 31% - в результате поиска в интернете - например, попадаются на обещания легкого заработка в сети. На телефонный канал здесь приходится только 16%, на прочие каналы - 21%. Средняя сумма потерь в этих каналах составляет: 5 500 руб. (соцсети), 14 500 руб. (поиск в интернете), 59 тыс руб (телефон), 13 600 руб. (объявления, мессенджеры, e-mail и т.д.).



**Распространенность схем мошенничества**

В 42% случаев, когда мошенники пытаются выманить у клиентов смс-коды и данные карт, они представляются службой безопасности сторонних банков - то есть не того банка, операции по карте которого они планируют совершить. В 25% случаев они представляются службой безопасности непосредственно банка, по карте которого впоследствии будут запрашивать информацию. 11% мошеннических случаев приходится на схемы с покупкой и продажей товаров в сети. 22% - на другие сценарии (инвестиции, комиссии за получение выигрыша, вознаграждения за опрос и т.д.)



52% случаев, когда клиенты российских банков переводят деньги добровольно, приходится на схемы с продажами товаров в сети. Например - мошенники направляют своих жертв на фальшивые платежные шлюзы при попытке провести сделку на крупных классифайдах.

Сценарии со звонками клиентам российских банков с подменой номера по данным на начало 2020 года резко сократились - их количество уменьшилось в 10 раз по сравнению с началом 2019 года и сейчас составляет около 5% от всех случаев с использованием социальной инженерии. На начало 2019 доля случаев с подменой номера от всей социальной инженерии составляла около 18-20%

**Средняя сумма мошенничества**

Средний чек успешного мошенничества на одного клиента (может включать в себя несколько операций) по итогам 2019 г составил 9 300 рублей. За год эта сумма сократилась на 13%.

Больше всего денег клиенты теряют, когда предоставляют данные карт и смс-коды - около 27 700 руб. Меньше всего мошенники крадут с помощью интернет-магазинов, которые не верифицируют клиентов — 4 300 рублей.



В 2019 году сумма мошенничества при утере/краже карты упала почти в два раза до 9 800 рублей. Это связано с тем, что банки внедряют новые технологии, а финансовая грамотность клиентов растет: они чаще устанавливают лимиты на операции, не носят карты совместно с пин-кодами, оперативно сообщают в банк о пропаже и несанкционированных операциях.

***Алексей Бакланов, руководитель управления противодействия мошенничеству и претензионной работы Тинькофф:***

*“В 2019 году выросла доля случаев с добровольными переводами мошенникам, доля остальных — упала. Этому есть несколько причин. Главное - банки учатся быстро реагировать и предотвращать хищения. Тинькофф внедряет новейшие технологии и адаптируется к агрессивной преступной среде.*

*Но у банков до сих пор недостаточно инструментов, чтобы помешать обманутым клиентам перевести деньги преступникам. Мошенники используют приемы психологического давления, из-за чего обманутый клиент самостоятельно переводит им деньги. Бывают случаи, что сотрудники банка посчитают операции подозрительными и свяжутся с клиентом для подтверждения, он может ввести их в заблуждение, действуя по указаниям мошенников. Клиент понимает свою ошибку, лишь когда деньги вернуть уже нельзя.*

*Какие технологии мы используем:*

***Machine Learning****. Тинькофф с помощью алгоритмов машинного обучения отслеживает нетипичные для клиента транзакции. Более 300 признаков могут показать, что операцию совершает не клиент. В этом случае с клиентом связывается служба безопасности. В прошлом году мы начали поэтапно внедрять машинное обучение в антифрод-систему и стали на 40% лучше предотвращать случаи мошенничества, когда клиент разглашает данные карты. Плюс на 35% мы снизили уровень “зря потревоженных клиентов”.*

***Технология цифрового отпечатка устройства (фингерпринт).*** *Идентифицирует устройство, с помощью которого клиент использует сервисы Тинькофф. Это позволяет определить, когда сервисами пользуется другой человек. На основании этих данных применяются дополнительные методы аутентификации платежей и входа в личный кабинет.*

***Кросс-канальный событийный мониторинг в режиме 24/7.*** *Антифрод система проверяет все операции клиентов в режиме реального времени. Она учитывает активность клиентов во всех каналах: в онлайн-банкинге, мобильном приложении, при оплате пластиковыми картами и пр. При подозрительных операциях служба безопасности банка связывается с клиентов в течение 1-2 минут.*

***Геолокация в антифрод-системе.*** *В рамках этой технологии для каждого клиента составляются облака доверенных координат — операции в этих областях считаются менее рискованными”.*

**Типичные схемы обмана**

***При добровольном переводе средств клиентом***

**Покупки в интернете.** Клиент находит объявление о продаже товара или услуг. Переводит деньги, мошенники перестают выходить на связь.

**Покупки в интернете с подменой формы**. Эта схема распространена при покупках на различных сайтах объявлений. Мошенники не просят перевести деньги за товар, а отправляют клиенту ссылку с формой на оплату - она вызывает больше доверия. Используя уязвимости в протоколе, мошенники подменяют название торговой точки. Клиент предполагает, что совершает покупку, но на самом деле переводит деньги на карту.

**«Близкий человек попал в беду».** В соцсетях пишет родственник или друг. Он попал в непростую ситуацию и ему срочно нужны деньги. Так действуют мошенники, взломав аккаунты.

***При разглашении банковских данных***

**Служба безопасности банка**. Клиенту поступает звонок или смс с просьбой перезвонить. Мошенники представляются службой безопасности банка, говорят, что зафиксирована попытка списания денег со счета клиента, выясняют данные карты и коды подтверждения и списывают деньги со счета.

**Лотерея или опрос**. Клиент видит рекламу в интернете или таргетированную рассылку: можно получить вознаграждение, поучаствовав в лотерее или пройти опрос. Для этого нужно заполнить небольшую форму. Клиент вводит данные карты — мошенники списывают средства, либо получают данные для последующих попыток обмана.

**Продажа в интернете.** Клиент размещает объявление о продаже товара. Мошенники звонят и узнают данные карты продавца под предлогом необходимости совершить перевод за товар. Далее они списывают деньги с карты, узнав у продавца код подтверждения (якобы он нужен для зачисления). Другой вариант этой схемы — использование подложного сервиса «безопасной сделки» в интернете.

**Нетипичные схемы обмана**

**Черные брокеры**. Клиенту поступает предложение заработать на инвестициях. Он связывается с лжеброкерами и переводит им деньги для игры на бирже. Сумма на «брокерском» счете начинает быстро расти. Клиент хочет вывести средства, но для этого нужно заплатить дополнительную комиссию. Он переводит деньги — мошенники пропадают.

**Программы удаленного доступа.** Звонит «служба безопасности банка»: на устройстве клиента обнаружен вирус, необходимо скачать антивирус и сканировать гаджет. Во время сканирования устройство, якобы, нельзя использовать, так как вирус может распространиться дальше. На самом деле клиент скачивает программу удаленного доступа, а во время «проверки» мошенники получают доступ к мобильному банкингу и выводят средства клиента.

**Безопасный счет**. Звонок от «службы безопасности»: произошла утечка данных, в ней замешаны сотрудники. Необходимо снять деньги через безопасный банкомат банка-партнера и перевести их на специальный страховочный счет.

Другим вариантом этой схемы является сценарий, когда преступники предлагают сразу перевести деньги на счет, не снимая их в банкомате. За причиненные неудобства клиенту предлагается вознаграждение. Мошенники просят не отключать телефонную связь во время операций. Предупреждают, что “банк” не несет ответственность за сохранность денег по условиям обслуживания счета: если их не снять, они могут пропасть.

**Знакомства в сети**. На сайте знакомств девушка предлагает сходить в кино. Отправляет ссылку на сайт-однодневку VIP-кинотеатра. Клиент покупает билеты, на этом знакомство завершается.

**Автоматическая голосовая служба банка.** Звонок из «банка»: был зафиксирован вход в личный кабинет из другого города или страны. В рамках мер по безопасности необходимо назвать номер карты для идентификации. Мошенники предупреждают, что сейчас поступит код по смс, но его никому нельзя называть. После чего переключают на голосовую службу. Клиент доверяет голосу робота и вводит код в тональном режиме. Мошенники меняют пароль и логин в его личном кабинете и выводят деньги.

**Базовые меры безопасности:**

**Нужно всегда держать в тайне следующие данные**: коды из смс и пуш-уведомлений, пин-код карты, контрольные вопросы, данные карты, включая срок действия и трехзначный код. Нельзя также раскрывать персональные данные: отчество, место и год рождения, данные паспорта.

**Если кто-то позвонил сам**, не следует ему доверять, даже если он представился сотрудником банка. Нужно перезвонить в банк в случае подозрительного звонка или сообщения от банка.

**Не нужно скачивать никакие программы на смартфон по просьбе незнакомцев** и тем более предоставлять им доступ к ним.

**Не нужно носить записанный пин-код рядом с картой**. Лучше подключить оповещения об операциях и настроить лимиты на траты.

Для быстрой связи с банком нужно заранее сохранить его номера в телефоне.

**Если карта пропала — нужно сразу же связаться с банком, заблокировать карту,** проверить операции и обратиться в банк для выпуска новой карты.

**Если украли деньги со счета — нужно связаться с банком и описать ситуацию**. После чего — написать заявление в полицию и отправить в банк талон о принятии заявления

**Если пропал телефон — нужно связаться с банком для блокировки приложения и удаления данных карты со смартфона**. Также нужно немедленно обратиться к сотовому оператору для блокировки сим-карты и проверить последние операции.

Подробнее о том, как защититься от мошенников можно прочитать на сайте [Tinkoff Secure](https://www.tinkoff.ru/secure/)

\*Исследование было составлено на основе данных клиентов Тинькофф, а также данных 400 000 клиентов российских банков из топ-30 по объему активов, в отношении которых предпринимались попытки успешного и неуспешного мошенничества в 2019 году.

**Контакты:**

Тинькофф

**Александр Леонов**

+ 7 495 648-10-00 (доб. 35738)

media@tinkoff.ru

**Экосистема Тинькофф**

Тинькофф — финансовая онлайн-экосистема, выстроенная вокруг потребностей клиента.

Экосистема Тинькофф предоставляет полный спектр финансовых услуг для частных лиц и для бизнеса. Особое внимание Тинькофф уделяет развитию лайфстайл-банкинга: экосистема дает клиентам возможность анализировать и планировать личные траты, инвестировать сбережения, получать бонусы в рамках программ лояльности, бронировать путешествия, покупать билеты в кино, бронировать столики в ресторанах и многое другое.

Все сервисы Тинькофф доступны через мобильные приложения и сайт Tinkoff.ru.

Тинькофф не имеет отделений: сеть собственных представителей позволяет доставлять продукты компании в любой регион страны в кратчайшие сроки, а клиенты обслуживаются через онлайн-каналы и контакт-центр. Во всех коммуникациях Тинькофф активно использует технологии искусственного интеллекта и машинного обучения, более 30% обращений клиентов в чатах обрабатывается без участия сотрудников банка.

Все продукты и большинство внутренних ИТ-систем Тинькофф разработаны самой компанией. 70% сотрудников штаб-квартиры — ИТ-специалисты.

Ядром экосистемы является основанный в 2006 году Тинькофф Банк — крупнейший независимый онлайн-банк в мире, обслуживающий более 10 миллионов клиентов. Банк был признан журналом Global Finance «Лучшим розничным онлайн-банком мира» (2018), «Лучшим розничным онлайн-банком России» (2015, 2016, 2018 и 2019 г.), «Лучшим розничным онлайн-банком в Центральной и Восточной Европе» (2019), журналом The Banker — «Банком Года России» (2013, 2017 г).

Материнская компания банка TCS Group Holding PLC торгуется на Лондонской фондовой бирже и на Московской бирже. Чистая прибыль TCS Group Holding PLC по МСФО за девять месяцев 2019 г. составила 25,1 млрд руб., рентабельность капитала — 59%.