

Как Казахстан защищает граждан от финансовых мошенников

Телефонные звонки от «сотрудников банка», фальшивые кредиты, украденные деньги и подставные банковские счета — схемы финансовых мошенников становятся все сложнее. Сегодня преступники используют не один способ обмана, а сразу несколько: психологическое давление, дистанционное оформление кредитов, вредоносные программы и целые цепочки счетов для вывода похищенных денег. Поэтому бороться с такими преступлениями можно только комплексно.

Современные методы защиты

За последние несколько лет в Казахстане появилось сразу **несколько механизмов защиты**: одни помогают не допустить оформления мошеннического кредита, другие позволяют вовремя остановить подозрительный перевод, а третьи защищают людей, которые уже стали жертвами злоумышленников.

Первые результаты уже заметны. Если в 2024 году было выявлено 8,7 тысячи мошеннических займов на сумму 20,3 млрд тенге, то в 2025 году – уже 5,1 тысячи на 4,6 млрд тенге. С начала 2026 года выявлено около 1,3 тысячи таких кредитов на сумму 2,1 млрд тенге.

Один из самых простых и одновременно самых эффективных способов защиты – **добровольный отказ от получения кредитов** (Стоп - кредит).

Через портал eGov любой человек может установить запрет на оформление банковских займов и микрокредитов на свое имя. После этого информация автоматически поступает в кредитные бюро, а затем – во все банки и микрофинансовые организации. Если при рассмотрении заявки действует такой запрет, кредит оформить нельзя.

Причем ответственность лежит не на клиенте, а на финансовой организации. Если банк или МФО все же выдадут кредит, несмотря на установленный запрет, такая задолженность должна быть списана.

Этим сервисом уже воспользовались более 6,5 миллиона казахстанцев, что делает его одним из самых востребованных инструментов защиты от мошеннических кредитов.

Большинство людей представляют мошеннический кредит как ситуацию, когда преступники каким-то образом получают доступ к чужим документам и самостоятельно оформляют заем. На практике гораздо чаще происходит другое.

Мошенники убеждают человека самому взять кредит. Они представляются сотрудниками банка, полиции, Комитета национальной безопасности или других государственных органов, сообщают о якобы попытке хищения денег и предлагают «спасти» средства. Под психологическим давлением человек самостоятельно оформляет заем, после чего переводит полученные деньги преступникам.

Чтобы дать человеку возможность спокойно оценить ситуацию и вовремя понять, что его пытаются обмануть, в Казахстане введен так называемый **период охлаждения**.

Теперь при оформлении крупных онлайн-кредитов деньги перечисляются **не сразу после подписания договора**. Если сумма кредита составляет от 649 тысяч до 1,1 млн тенге, банк обязан выдержать паузу **не менее 8 часов**. При еще более крупных банковских кредитах и онлайн-микрокредитах этот срок составляет уже не менее суток.

За это время финансовая организация проводит дополнительную проверку на наличие признаков мошенничества, а клиенту необходимо **повторно подтвердить** свое желание получить кредит. Если появляются основания полагать, что человек действует под влиянием злоумышленников, выдача денег может быть приостановлена.

Еще одна мера касается граждан, которые **впервые оформляют крупный беззалоговый кредит**. Если кредитной истории раньше не было, получить такой заем дистанционно уже нельзя. Для этого потребуется лично посетить отделение банка и пройти биометрическую идентификацию. Это значительно снижает риск оформления крупных кредитов на человека без его ведома.

Дополнительная защита действует и для отдельных категорий граждан. Если заемщик младше 21 года или старше 55 лет, оформить онлайн-кредит можно только после получения специального согласия через портал eGov, кредитное бюро или банковское приложение, интегрированное с государственными сервисами.

Такой дополнительный этап помогает убедиться, что человек действительно осознает свои действия и самостоятельно принимает решение о получении кредита.

Оценка поведения и биометрия

Для дополнительной защиты банки сегодня оценивают не только документы клиента, но и обстоятельства оформления займа. Если клиент заметно нервничает, постоянно разговаривает по телефону, получает чьи-то указания или не может объяснить, зачем берет кредит, это может быть признаком мошеннического воздействия.

Кроме того, банки обмениваются информацией о кредитных заявках. Если человек уже оформляет кредит в одной финансовой организации, получить еще один заем одновременно в другой не получится. Это помогает предотвратить ситуацию, когда мошенники пытаются заставить жертву взять сразу несколько кредитов.

Как мера дополнительной защиты всех финансов – **обязательная биометрия**. Кроме того, и кредит оформить онлайн без подтверждения личности невозможно. Помимо электронной цифровой подписи используется обязательная биометрическая идентификация, которая помогает убедиться, что кредит оформляет именно владелец документов.

Банки также используют дополнительные инструменты защиты. Они проверяют устройство, с которого подается заявка, фиксируют подозрительную активность, распознают попытки удаленного управления телефоном и могут приостановить операцию, если замечают признаки мошенничества.

Все эти меры позволяют выявить подозрительную активность еще до того, как деньги будут перечислены.

Как Антифрод-центр помогает остановить мошенников

С июля 2024 года в Казахстане работает Антифрод-центр Национального Банка. Это единая система, которая объединяет банки, операторов связи и правоохранительные органы.

Если один из участников обнаруживает подозрительную операцию, информация практически сразу становится доступна остальным. Это позволяет быстрее выявлять мошеннические переводы, устанавливать счета, через которые проходят похищенные деньги, и блокировать их до того, как средства будут выведены.

При необходимости банки могут временно приостановить подозрительный перевод на срок до пяти рабочих дней, чтобы проверить его законность. Такая пауза помогает сохранить деньги клиента, если есть основания полагать, что перевод совершается под влиянием мошенников.

В настоящее время в Антифрод-центре Национального Банка зарегистрировано более 180 тыс. инцидентов. В рамках борьбы с мошенничеством банками самостоятельно за период с начала 2025 года по 1 мая т.г. было предотвращено около 163 тыс. мошеннических операций на сумму более 68 млрд тенге. При этом по информации Антифрод-центра Национального Банка предотвращено и заблокировано мошеннических и незаконных операций на сумму более 28,9 млрд тенге.

Чтобы усложнить работу телефонных мошенников, в Казахстане усиливаются требования к регистрации SIM-карт и борьбе с так называемыми серыми номерами.

Теперь один человек может зарегистрировать ограниченное количество SIM-карт, а для оформления новой требуется пройти биометрическую идентификацию. Кроме того, операторы связи выявляют и блокируют оборудование, которое позволяет подменять зарубежные номера казахстанскими.

Операторы связи обязаны внедрять собственные антифрод-системы, интегрированные с базами IMEI-кодов и абонентских данных, выявлять подозрительный трафик и блокировать номера, используемые в мошеннических схемах.

В результате уже заблокировано более 142,1 млн звонков и свыше 310 тыс. абонентских номеров с признаками мошенничества.

Еще одно направление борьбы связано с **дропперами** – людьми, которые за вознаграждение передают мошенникам свои банковские карты или счета для перевода похищенных денег.

Сегодня банки анализируют подозрительные переводы и могут выявлять счета, через которые проходят средства от большого количества отправителей или быстро переводятся дальше. Если

операция вызывает подозрения, банк вправе ограничить ее проведение, заблокировать карту и передать информацию в правоохранительные органы.

При этом дропперы рискуют не только административными или уголовными последствиями. Если через их счета проходили похищенные **деньги, пострадавшие могут потребовать их возмещения в судебном порядке.**

Что делать, если мошенники все же оформили кредит

Если гражданин стал жертвой мошенников и по этому факту возбуждено уголовное дело, банк или микрофинансовая организация обязаны приостановить начисление процентов, штрафов и пени. На время расследования также **прекращается взыскание задолженности.**

Если выяснится, что финансовая организация нарушила обязательные требования безопасности – например, проигнорировала добровольный отказ от получения кредита, не провела биометрическую идентификацию или не соблюла период охлаждения, – **задолженность подлежит списанию без обращения в суд.**

В более сложных случаях, связанных со взломом устройств, кражей персональных данных или использованием вредоносных программ, вопрос может решаться в судебном порядке.

Главное – при первых признаках мошенничества как можно быстрее обратиться в банк и правоохранительные органы. Чем раньше начнется проверка, тем больше шансов защитить свои права и предотвратить дальнейшие потери.