KMF

# ФИНАНСОВАЯ И ЦИФРОВАЯ БЕЗОПАСНОСТЬ

## КАК НЕ СТАТЬ ЖЕРТВОЙ ФИНАНСОВЫХ МОШЕННИКОВ

KMF-ДЕМЕУ

# СОДЕРЖАНИЕ

## ВИДЫ ФИНАНСОВОГО МОШЕННИЧЕСТВА



## ЧТО НУЖНО ЗНАТЬ ПРО БЕЗОПАСНЫЕ КРЕДИТЫ



*ВАЖНО: схемы мошенничества постоянно обновляются и совершенствуются, применяются новые современные технологии.



# ПРЕДИСЛОВИЕ

**Дорогой друг!**

Вы держите в руках брошюру, созданную в рамках проекта KMF и KMF-Демеу по повышению финансовой грамотности населения при сотрудничестве с Агентством Республики Казахстан по регулированию и развитию финансового рынка в рамках обучающего проекта **fingramota.kz**. Материалы, собранные в брошюре по финансовой и цифровой безопасности, помогут вам защитить себя от разных видов финансового мошенничества, распространенных в Казахстане и не только. Мы надеемся, что, ознакомившись с советами экспертов, вы не столкнетесь с такими ситуациями. Берегите себя, свои персональные данные и регулярно повышайте свою финансовую грамотность!

# 1. КАКИЕ ВИДЫ ФИНАНСОВЫХ МОШЕННИЧЕСКИХ СХЕМ РАСПРОСТРАНЕНЫ В КАЗАХСТАНЕ?

## ИНТЕРНЕТ-ЛОВУШКИ

Сейчас мошенники активно используют Интернет. Например, в сфере онлайн-торговли исключается непосредственный контакт с жертвой. Аферист публикует в соцсетях объявление о продаже какого-то товара. Покупателю говорит, что вещь будет доставлена только после стопроцентной предоплаты. Доверчивые клиенты перечисляют деньги, не подозревая, что ни товара, ни денег они не получат.

## НЕЗАМЕДЛИТЕЛЬНО ОБРАЩАЙТЕСЬ В СВОЙ БАНК, ЕСЛИ:

- Вы заметили необычную активность на своих счетах
- Вы не смогли получить удаленный доступ к своим счетам
- Вашу карту не приняли к обслуживанию
- Вы обнаружили в своей кредитной истории займы, которые не оформляли

## АФЕРЫ С НЕДВИЖИМОСТЬЮ

Например, мошенники предлагают покупателю приобрести залоговую квартиру по низкой цене, но при одномоментной выплате ее стоимости. При этом заключенный договор купли-продажи не дает покупателю гарантий на владение жильем.

Есть еще один вариант аферы – покупка квартиры по предоплате по очень выгодному предложению в интернете. Но после того, как покупатель внес аванс, "продавца" уже невозможно найти. Иногда мошенники снимают квартиру в аренду, а доверчивым покупателям представляются владельцами и продают им жилье. Чаще всего мошенники в поисках быстрой выгоды предлагают жертве внести аванс прямо сейчас, чтобы оставить за ним недвижимость.



## ФИКТИВНЫЕ КРЕДИТЫ

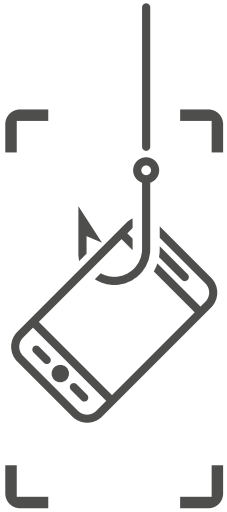
Если ваши документы были утеряны, срочно обращайтесь:

- в ЦОН, где ваши пропавшие документы аннулируют и предоставят соответствующие справки;
- в органы внутренних дел с заявлением об утере, где вам предоставят официальную справку с указанием времени и даты обращения. Таким образом в дальнейшем можно доказать свою непричастность к получению кредита.

## КАКИЕ ЕЩЕ МЕТОДЫ МОГУТ ПРИМЕНИТЬ МОШЕННИКИ?

*ОФОРМИТЬ НА ИНОЕ ЛИЦО*
*НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА*
*ПО ПОТЕРЯННОМУ ДОКУМЕНТУ.*

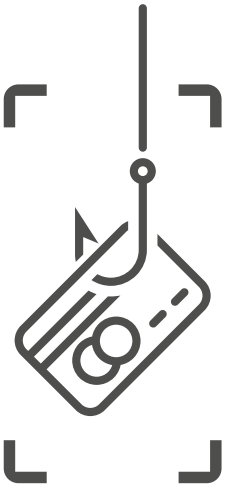




В кредитных организациях, где необходимо подтверждение согласия на получение кредита посредством SMS или иной идентификации номера мобильного телефона, мошенники могут оформить кредит, который будет подтвержден не только удостоверением личности пострадавшего гражданина, но и оформленным на него номером мобильного телефона.

***В этой связи желательно регулярно проверять у операторов мобильной связи наличие иных номеров, оформленных на вас.***

## *ВЫМАНИТЬ У ФИЗИЧЕСКИХ ЛИЦ ЛИЧНЫЕ ДАННЫЕ:*



копии документов, номера телефонов, в том числе родственников и адреса проживания. Для этого создаются лже-рекрутинговые агентства или просто организации, якобы предлагающие работу. При оформлении они требуют от гражданина полный пакет документов, который в дальнейшем передают другим лицам для совершения мошеннических действий. ***Необходимо заранее проверять информацию о потенциальном работодателе и передавать документы и личные данные только при заключении договора.***

## *ЗАПИСЬ ТЕЛЕФОННЫХ РАЗГОВОРОВ*

для якобы подтверждения удаленной идентификации. При этом мошенники звонят жертве и инициируют максимально возможное количество вопросов, на которые просят отвечать “да”, “согласен”, “подтверждаю” и прочее. В дальнейшем запись разговора, а точнее ответы могут быть использованы в качестве доказательства намерения получения кредита. ***Поэтому если вы не уверены в собеседнике, то просто прекратите с ним разговор и не давайте однозначных ответов.***



**В случае подозрения или выявления мошеннических схем важно обратиться в правоохранительные органы, так как поиск и привлечение к ответственности мошенников находится в их компетенции.**

**Чтобы не стать жертвой мошенников, не стоит оставлять без присмотра свои документы, старайтесь не отдавать их под залог для получения товаров или услуг в аренду, прокат.**

- Никогда и ни при каких обстоятельствах не озвучивайте и не отправляйте незнакомым людям свои персональные данные, включая копии документов, удостоверяющих личность.
- Не принимайте участие в сомнительных интернет-конкурсах и лотереях, в которых требуется предоставить персональную информацию.
- Никогда не передавайте и не публикуйте, в том числе в социальных сетях, реквизиты платёжной карты.
- Регулярно проверяйте свою кредитную историю, чтобы отследить наличие так называемых "подставных", фиктивных кредитов.

## ЗАПОМНИТЕ!

Настоящие представители финансовых организаций *никогда* не попросят вас сообщить реквизиты счетов и банковских карт, PIN-коды, CVV-коды и другую конфиденциальную информацию. Если у вас запрашивают такую информацию, сообщите об этом факте по горячей линии финансовой организации, а также обратитесь в ближайшее отделение банка или другой финансовой организации, в которой вы обслуживаетесь.



## НЕСКОЛЬКО РЕАЛЬНЫХ СЛУЧАЕВ МОШЕННИЧЕСТВА,

актуальных на сегодняшний день, а также простые правила поведения, которые помогут обезопасить ваши деньги.

### *ПРИМЕР* №1

*Вы потеряли или, что хуже, у вас украли мобильный телефон. Мошенники могут снять деньги либо совершить оплату с ваших счетов путем регистрации в интернет-банкинге по номеру украденного телефона или попросту зайти в уже установленный мобильный банкинг или мобильное приложение.*

В первую очередь необходимо заблокировать свои счета, обратившись в call-центр банка или ближайшее отделение банка, а также через Интернет-банкинг. Параллельно необходимо заблокировать номер украденного телефона через мобильного оператора.

### *ПРИМЕР* №2

*Потенциальной жертве звонят якобы сотрудники банка, заявляя, что обнаружили подозрительные операции по банковской карте и с целью их предотвращения просят указать ряд реквизитов: ИИН, номер телефона, к которому привязана карта, номер банковской карты, номер текущего или сберегательного счета. При этом они оказывают постоянное психологическое давление, говоря, что в случае, если не предоставить им данные, все деньги будут потеряны моментально.*

Что же делать в такой ситуации? Повесьте трубку и позвоните в банк, который вас обслуживает, для уточнения информации с мобильного телефона, а еще лучше посетите ближайшее отделение вашего банка

и напишите официальное заявление о попытках совершения атак на ваши счета. Ни в коем случае не продолжайте диалог со злоумышленниками и не сообщайте им никакую информацию.

Существует регламент действий сотрудников банков, в соответствии с которым сотрудники банков никогда не звонят клиенту первыми и не выставляют требования предоставить данные по карте, личные данные либо полученные по SMS. Любое общение по данным вопросам инициируется исключительно клиентом.

## *ПРИМЕР* №3

*Мошенники создали клон популярного интернет-магазина, сайта банка либо социальной сети с целью получения реквизитов ваших платежных карт, так называемый фишинговый сайт. Ссылки на него распространяются через имеющуюся базу почтовых адресов, в числе которых может оказаться и ваш адрес.*

Чтобы не попасть на уловки интернет-мошенников, помните несколько правил:

- нигде не указывайте ваши персональные данные;
- обращайте внимание на оформление сайта;
- проверяйте правильность ссылки в адресной строке;
- пользуйтесь защищенным соединением **https**;
- фильтруйте подозрительные письма;
- не пользуйтесь открытыми точками доступа wi-fi для входа в банковские аккаунты;
- обращайте внимание на форму оплаты. В надежных интернет-магазинах она открывается в новом окне и имеет верификацию одной из платежных систем (VISA, Mastercard).



# 2. ФИНАНСОВЫЕ ПИРАМИДЫ

### КЛАССИЧЕСКАЯ СХЕМА ПОНЦИ*

Это схема привлечения денег, которую используют большинство финансовых пирамид, согласно которой вложения привлекаемых в схему участников направлены на выплаты раннее привлеченных участников.

### ПОД ВИДОМ СЕТЕВОГО МАРКЕТИНГА

Это одна из наиболее часто используемых мошенниками схем для маскировки своей деятельности, имеющая схожие процессы с сетевым маркетингом. И сетевой маркетинг, и финансовые пирамиды имеют иерархическую структуру, программу по привлечению населения (“маркетинговый план”), выплату бонусов от продажи продукции или услуги (в случае пирамид это маскировка) и т. д. Основным отличием является то, что бонусы, различные выплаты при сетевом маркетинге включены в стоимость продукции, тогда как в пирамидах продукция или услуга необходимы для маскировки и открытого привлечения населения, а для того чтобы участник мог заработать, ему необходимо привлекать определенное количество клиентов, которые также приобретают товар на ту же сумму. Каждый привлеченный участник в свою очередь также привлекает дополнительно определенное количество участников и т. д.

### ПОД ВИДОМ ОНЛАЙН-ИГР

Мошенники могут рассылать информацию в интернете, привлекая граждан возможностями заработка, участием в играх в онлайн-группах в социальных сетях и другое. Примерами таких схем являются “Котел”, “Черная Касса”. Гражданам предлагают вступить в группу,

* Чарльз Понци — итальянский “пирамидостроитель”, основатель “схемы Понци”, создатель одной из самых хитроумных и оригинальных финансовых пирамид, которая потом была названа в его честь.

осуществлять регулярные взносы и получить в короткие сроки высокий доход. При этом необходимо привлекать дополнительных участников. Взносы осуществляются на карточные счета организаторов. Данные суммы впоследствии снимаются со счетов в наличной форме или переводятся на счета в других банках, а организаторы скрываются.

## ПОД ВИДОМ ПРЕДОСТАВЛЕНИЯ РАЗЛИЧНЫХ ТУРИСТСКИХ УСЛУГ

Организаторы предлагают получить высокий доход путем привлечения участников, к примеру, в круизные клубы. Проводятся всевозможные семинары, курсы, обучение участников. Но необходимо осуществление регулярных взносов и привлечение новых участников. Зачастую компании, предлагающие туристские услуги и привлекающие денежные взносы, не зарегистрированы на территории Казахстана.

## ОНЛАЙН-КРЕДИТОРЫ (МОШЕННИЧЕСТВО)

Недобросовестные компании, зарегистрированные за рубежом, предлагают получение займов с низкой ставкой вознаграждения. Клиент указывает свои банковские реквизиты, после чего возможны несколько сценариев развития событий:

- Клиенту не выдают заем, вместо этого на ежемесячной основе списывается сумма за подписку. В случае если на карточке отсутствует необходимая сумма, то сумма списывается сразу после пополнения счета.
- Клиенту выдается заем, но сумма намного меньше, чем указана в договоре, тогда как вознаграждение начисляется на сумму договора. Это объясняется тем, что имеются скрытые комиссии, наличие страховки и т. д.
- Клиенту выдается сумма, но имеются скрытые отчисления, такие как высокая ставка вознаграждения, комиссии по просрочке, штрафы, пени и т. д.



При этом, согласно Закону РК "О микрофинансовой деятельности", выдача микрокредитов возможна только после прохождения учетной регистрации в уполномоченном органе. Следует проверять данную информацию на сайте **finreg.kz**.

## ПОД ВИДОМ ТОРГОВЛИ FOREX

Клиенту предлагают консультационные услуги, а также прохождение обучения по торговле на специальных платформах. В процессе обучения клиенту предлагают попробовать осуществлять операции на демоверсии торговой площадки, своего рода тренинговые версии. В последующем клиенту предлагают внести деньги для осуществления реальной торговли. Мошенниками используются платформы, которые не позволяют заработать деньги, а лишь создают видимость кратковременного заработка. В итоге клиент не получает обещанный доход.

## РАЗЛИЧНЫЕ ИНВЕСТПРОЕКТЫ

Данная мошенническая схема основана на привлечении денежных средств для инвестиционной деятельности. Физические лица и компании предлагают высокую доходность в короткие сроки при осуществлении инвестирования в определенные проекты. При этом, в случае если клиент пригласит дополнительно 2 человек и более, доход клиента может увеличиться.

## ПОТРЕБИТЕЛЬСКИЕ КООПЕРАТИВЫ

Потребительский кооператив является объединением граждан, которое помогает в удовлетворении потребностей членов кооператива, с более выгодными условиями в сравнении с другими организациями (пример, ипотека банка). Организаторы предлагают приобрести недвижимость в короткие сроки с минимальным первоначальным взносом, в случае привлечения дополнительно новых участников, сумма первоначального взноса снижается. Таким образом, привлекается большое количество граждан, недвижимость не приобретается,

а организаторы скрываются. Также имеют место случаи, когда компании привлекают инвестиции на периодичной основе на более долгий срок, доход также формируется от вложений дополнительно привлеченных лиц.

## ДОГОВОР ПРОСТОГО ТОВАРИЩЕСТВА

Одним из новых видов мошенничества является заключение договора займа под видом участия в простом товариществе. Данное мошенничество осуществляется по следующему принципу: мошенники предлагают получить заем, вне зависимости от кредитной истории, возраста и т. д. Условием выдачи займа является вступление в простое товарищество. Возврат суммы долга вуалируется под выкуп участником доли в простом товариществе, при этом сумма долга в несколько раз превышает сумму, выданную в качестве займа. Необходимо помнить, что микрокредитование осуществляют организации, имеющие лицензию Агентства. Также следует отметить, что зачастую жертвами таких недобросовестных действий становятся пожилые и молодые люди. Будьте осторожны!

## ФАНДРАЙЗИНГОВЫЙ ФОНД

Данный вид мошенничества чаще используется в западных странах, но в последнее время имелись случаи и в Казахстане. Суть заключается в том, что корпоративный фонд представляет платформу, на которой физические лица могут предоставлять займы другим физическим лицам. Однако суть мошенничества заключается в том, что под видом корпоративного фонда или иных фондов организаторы предоставляют займы населению в соответствии со своими условиями. После заключения договора займа данная организация предлагает инвестировать деньги в проекты для получения гарантированной высокой прибыли.

## ПОД ВИДОМ ВЫДАЧИ КРЕДИТОВ

Работает схема по принципу Понци, но в качестве вознаграждения организация выдает своим участникам займы. Для получения участником большой суммы займа требуется внести определенную сумму денег и привлечь дополнительно нескольких участников, которые в свою очередь также внесут необходимую сумму денег. Организаторы обещают выдать заем после того, как наберется необходимая сумма денег от привлечения участников.

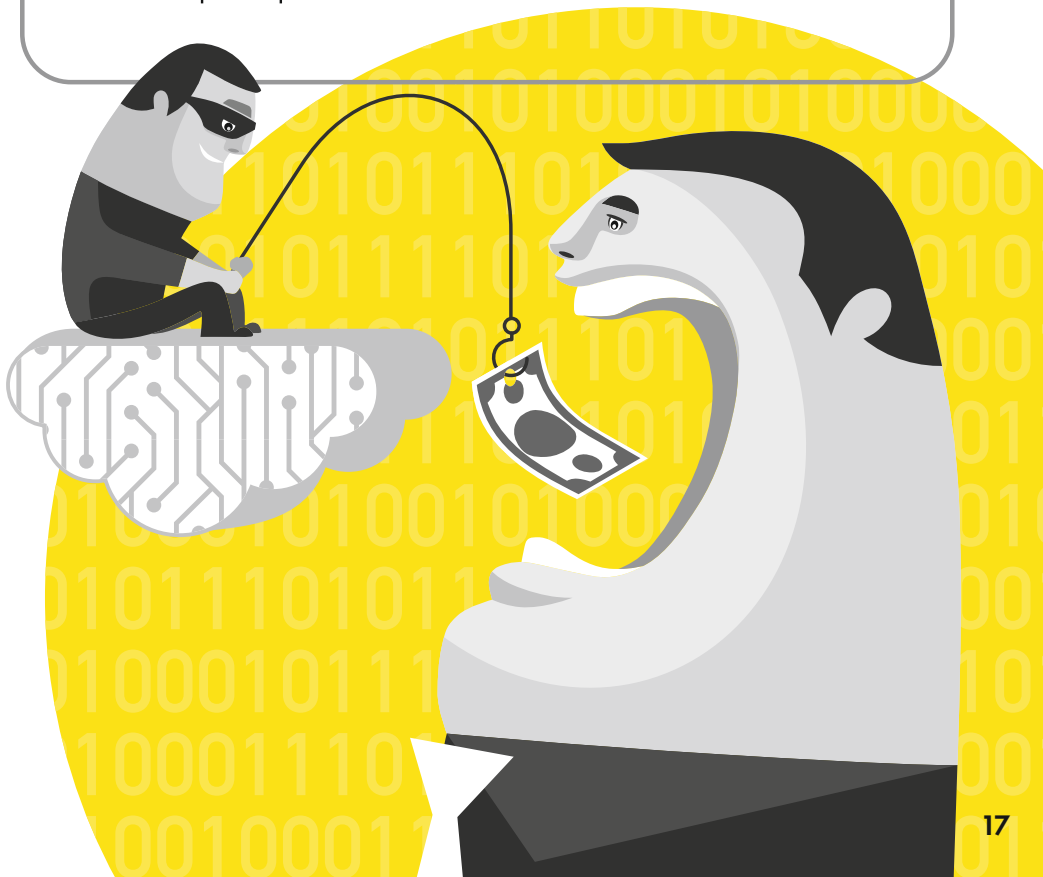
## ПОД ВИДОМ ПОГАШЕНИЯ ОБЯЗАТЕЛЬСТВ

Данная схема используется мошенниками при наличии у лица кредитов либо иных обязательств перед юридическими и физическими лицами. Мошенники предлагают заемщику “решить” вопрос или взять обязательства по оплате кредита на себя. Для этого заемщику необходимо оплатить часть от суммы кредита (от 10% до 40%). К примеру, если у заемщика имеется задолженность по кредиту в размере 300 тыс. тенге, то оплатив 50 тыс. тенге данным лицам, предложившим “решить вопрос”, заемщик якобы погашает всю сумму займа. В действительности мошенники запрашивают дополнительные суммы средства для решения вопроса. В итоге задолженность клиента не погашается, при этом возрастают расходы (штрафы, пени и т.д.).

**В НАСТОЯЩЕЕ ВРЕМЯ ФИНАНСОВЫЕ ПИРАМИДЫ СТАЛИ НАИБОЛЕЕ АКТИВНЫМИ В СОЦИАЛЬНЫХ СЕТЯХ**

## СТРАНИЧКА ВМЕСТО САЙТА

Чтобы создать сайт, надо его сначала разработать, сверстать, разместить на сервере, заплатить за хостинг, а главное – *зарегистрировать*. Чтобы создать страничку в социальной сети, нужен номер телефона или аккаунт электронной почты. Анонимность и децентрализованность позволяют мошенникам оставаться в относительной безопасности и продвигать свои схемы практически безнаказанно. Достаточно создать в социальной сети образ успешного человека с большим опытом в бизнесе и "накрутить" пару тысяч подписчиков и все – вы гуру инвестирования, бизнес-коуч, гений, миллиардер и филантроп в одном лице. К сожалению, некоторые пользователи, особенно молодые, верят, что можно быстро и безболезненно разбогатеть. Этому способствуют фейковые истории успеха и демонстрация "красивой" жизни: яхты, кабриолеты, песчаные пляжи и дорогое шампанское – все это рядом, только инвестируй в этот "крайне успешный и динамично развивающийся проект". Однако, как показывает практика, вкладчики не только не получают обещанную доходность, но и теряют уже вложенные в такие проекты средства. Возникают и ситуации, когда мошенники сначала выплачивают небольшое вознаграждение (которое, кстати, формируется исключительно за счет вновь приходящих вкладчиков) и предлагают в дальнейшем тем больший процент, чем больше средств вы вложите. Такие "стимулирующие выплаты" заставляют пользователей не только вложить все имеющиеся средства, но и иногда продавать имущество и даже брать кредиты.



# 3. ВИШИНГ: КОГДА АТАКУЮТ ТЕЛЕФОННЫЕ МОШЕННИКИ


## ВИШИНГ –

***(англ. vishing – от voice phishing) — метод мошенничества, когда злоумышленники, используя телефонную коммуникацию и играя определённую роль (сотрудника банка, покупателя) под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом или платежной картой.***



## ЭТО ВАЖНО ЗНАТЬ ПОТРЕБИТЕЛЯМ ФИНАНСОВЫХ УСЛУГ!

Одним из распространенных способов кражи средств со счетов граждан является телефонное мошенничество, или вишинг. Финансовые мошенники используют систему голосовой биометрии, чтобы атаковать клиентов. К примеру, представляясь службой безопасности одного из казахстанских банков, мошенники задают такие вопросы, которые подразумевают только положительный ответ – "Да". Допустим, живете ли вы в Алматы? Или называет ваши имя, фамилию и спрашивает, вы ли это. Также мошенники просят клиентов по телефону назвать три цифры на обороте платежной карты, якобы для идентификации. Или просят клиентов медленно и четко проговорить код из SMS-сообщения. Важная информация, озвученная вашим голосом, может стать тем самым паролем или подтверждением для получения, например, онлайн-займа или снятия денег с вашей карточки.

## КАК БЫТЬ В ТАКИХ СЛУЧАЯХ?

### СОВЕТ № 1

**Лучше невежливо прервать разговор, чем вежливо сообщить PIN-код карты.**

Даже старые проверенные методы мошенников работают безотказно. Самый простой развод: звонит якобы сотрудник банка. Он тревожно сообщает, что по вашей карте пытаются провести транзакцию. И если это не вы, то вам необходимо срочно предоставить звонящему всю информацию по своей карте. В таком случае лучше сразу прервать разговор и положить трубку. Сотрудник банка никогда не запросит эти данные и первым не позвонит. Для того чтобы убедиться в том, что к вам позвонили финансовые мошенники, необходимо позвонить в банк, в котором вы обслуживаетесь. Но ни в коем случае не на тот номер, с которого поступил звонок.

## СОВЕТ №2

**Не спешите раскрывать первому звонящему свои данные, поскольку в банке их и так знают.**

Настоящему банковскому менеджеру нет нужды звонить вам, чтобы уточнить вашу фамилию, паспортные данные, какие карты были оформлены, сколько денег на них осталось. В банке имеется ваше полное финансовое досье – кредитная история. Поэтому с этими вопросами сотрудники банка по телефону **НИКОГДА** к вам не обратятся. Эта информация представляет ценность только для мошенников.

## СОВЕТ №3

**Имейте в виду, банки никогда не звонят сами, чтобы спросить по телефону у клиентов:**

- полный номер карточки,
- срок ее действия,
- CVC/CVV,
- логин и пароль к интернет-банкингу,
- кодовое слово, код из SMS-сообщения.

Эти данные банк может запросить только в том случае, если вы сами позвонили туда, чтобы решить какой-то вопрос. Например, записаться на прием, разблокировать карту при поездке за рубеж, уточнить, где можно забрать перевыпущенную карту и т. п. Если же вам звонят и, представляясь сотрудником банка, запрашивают такую информацию, то можно не сомневаться – это мошенники.

## СОВЕТ №4

**Не поддавайтесь панике, если вас попытаются запугать телефонные мошенники.**

На паническое заявление о том, что с вашей картой серьезная проблема лучший ответ: “Сейчас позвоню или схожу в банк, чтобы проверить это лично”. Будьте уверены – звонящий тут же отключится. Это очень распространенная уловка – напугать владельца карточки. Ситуации могут быть придуманы разные:

- “Кто-то проводит подозрительные транзакции по вашей карточке”
- “Срочно! Уже списана энная сумма с вашего счета или карточки, чтобы спасти остаток, надо деньги перевести на временный счет”
- “Это вы пять минут назад подали заявку на оформление кредита? Если нет, то срочно нужны ваши данные, чтобы отменить ее”
- “Ваша карточка заблокирована, чтобы ее разблокировать на ваш телефон придет SMS, в котором указан код, назовите его” и т. д. Главная цель мошенников – напугать вас.

Стоит помнить, что если с вашей картой действительно какие-то проблемы, то банк может сам ее заблокировать и, скорее всего, пришлет об этом уведомление по оговоренному в договоре каналу – на электронный адрес, SMS. Причем с известного вам короткого номера или электронного адреса. И помните: любые подобные вопросы нужно прояснять и решать в отделении банка, но никак не по телефону. Поэтому, если мошенники идут ва-банк, вы идите в банк!

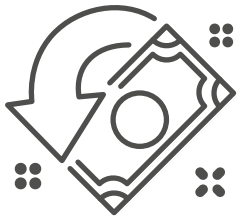
## СОВЕТ №5

**Помните, что псевдопризы и выигрыши – любимые “троянские кони” мошенников.**

С завидным постоянством на телефоны приходят сообщения о призах и выигрышах со ссылками, по которым можно узнать, как их получить. Как бы ни было сильно любопытство, не переходите по ним. Это уже классический прием – своего рода “троянский конь”, который, едва вы перейдете по этим ссылкам, “внедрит” в смартфон вредоносное программное обеспечение, чтобы выкрасть конфиденциальную информацию.

Устоять перед соблазном получить выигрыш сложно, учитывая, что внешне такие лжесообщения трудноотличимы от реальных сообщений банков, операторов связи или известных торговых центров. Мошенники обычно используют сервисы по сокращению интернет-ссылок, и выявить подвох становится сложно.
Поэтому, если вы получили сообщение о выигрыше, то, прежде чем переходить по ссылке, уточните, был ли такой розыгрыш в действительности. А лучше – просто удалить такое SMS-сообщение.

## ВЫСОКИЕ КЭШБЭКИ



Еще один способ – это высокие кэшбэки. Телефонные мошенники звонят клиенту и, представляясь сотрудниками банка, в котором он обслуживается, предлагают ему воспользоваться их кэшбэк-сервисом. К примеру, злоумышленники предлагают выпустить карту с высоким и гибким кэшбэком от 8%  до 30%, который действует на покупки во всех розничных сетях. Обслуживание у такой карты, как правило, бесплатное, срок выпуска минимальный: от 1 до 3 дней, доставка карты может быть бесплатной, учитывая усиление карантинных мер. Если клиент отвечает утвердительно, то псевдоменеджер просит после звукового сигнала оценить его работу от 1 до 10, затем переключает на операциониста, при этом для пущей убедительности играет мелодия банка для ожидания на линии. Новый оператор уточняет все детали, когда будет удобно привезти карту или с какого отделения удобнее ее забрать, перепроверяет данные клиента и, внимание, просит назвать код для подтверждения выпуска карты, который приходит клиенту посредством SMS. Оператор просит отвечать на вопросы быстро, не давая клиенту времени сосредоточиться и тем самым усыпляя его бдительность. После того, как нужные данные получены, оператор завершает разговор и также просит оценить его работу по десятибалльной шкале. Ничего не подозревающий клиент впоследствии недосчитывается денег с карты, снять которые мошенникам не составляет особого труда.



К слову, код, который клиент называет оператору, на самом деле способствует активации приложения личного кабинета клиента банка. Мошенники таким образом получают управление банковским счетом, совершая переводы и иные транзакции, они могут отключить SMS и push-уведомления, и тогда клиент не сразу узнает о пропаже своих средств.

Имейте в виду, что настоящему банковскому менеджеру нет нужды звонить, чтобы уточнить информацию о вас: фамилию и паспортные данные, оформленные карты и их реквизиты, а также остатки денежных средств. В банке имеется ваше полное финансовое досье и кредитная история. Поэтому с этими вопросами сотрудники банка по телефону никогда не обратятся. Эта информация представляет ценность только для мошенников. И уж тем более сотрудники банка не будут запрашивать у вас те данные ваших банковских карт, которые необходимы для осуществления операций и оплаты. Даже в SMS, приходящих от некоторых автоматизированных банковских систем, указано: “Не передавайте коды никому, даже сотрудникам банка”.

# ВНИМАНИЕ, ФИШИНГ!

Фишинг – это вид интернет-мошенничества, когда злоумышленники “выуживают” конфиденциальные данные пользователей. Для этого мошенники используют такие инструменты, как фишинговые сайты, e-mail рассылки, всплывающие окна, таргетированную рекламу.

Интернет-аферисты могут опустошить ваш счет за считанные секунды, особенно если вы попадете на фишинговый сайт. Это одна из разновидностей финансового мошенничества, когда злоумышленники создают клон, к примеру, популярного интернет-магазина, сайта банка либо социальной сети с целью получения реквизитов платежных карт. И распространяют ссылки на него через имеющуюся базу почтовых адресов, в числе которых может оказаться и ваш адрес.

Чтобы знать, как бороться с фишинговыми сайтами, необходимо иметь минимальные знания об Интернете, его использовании и методах защиты информации. Так, если речь идет об интернет-магазине, к примеру, то убедитесь, что его адрес начинается с **https://**, а не с **http://**. Даже если вы не распознали фишинг с первого взгляда, есть простые базовые правила, которые позволяют не угодить в финансовую ловушку.



Первое, что должно насторожить, если вы на сайт все-таки прошли – предложение ввести свои персональные данные, в т. ч. реквизиты платежных карт, включая CVV-код (трехзначный номер на тыльной стороне карты). Уже на этом этапе нужно остановиться и немедленно покинуть сайт, сменив затем пароль.

Чтобы не попасть на уловки кибермошенников, запомните несколько правил: нигде не указывайте свои персональные данные, обращайте внимание на оформление сайта, проверяйте правильность ссылки в адресной строке, пользуйтесь защищённым соединением **https**, фильтруйте подозрительные письма, не пользуйтесь открытыми точками доступа wi-fi для входа в банковские аккаунты. Никому не сообщайте свои конфиденциальные данные: паспортные данные, реквизиты перевода (особенно секретный код перевода).

# ПРОМОКОД – НЕ ВСЕГДА СКИДКА!

Другой похожий метод мошенничества также основан на фишинге. Но предлагают вам не розыгрыши и призы, а скидки и промокоды. В этом случае фишинговые сайты выглядят как сервисы, на которых можно найти и купить скидочные купоны на различные товары и услуги. Учитывая развитие современных сервисов, от доставки до выполнения различных работ онлайн, промокоды уже ни у кого не вызывают подозрения и активно используются всеми. Наиболее популярны они в молодежном сообществе, где опять же активно используется схема "приведи друга – получи скидку". Поэтому распространяется информация о таких сервисах очень быстро.

Собрав достаточное количество данных банковских карточек и персональных сведений о пользователях, мошенники прекращают работу фишингового сайта и создают новый. Все это для того, чтобы максимально "замести следы".

Поэтому, прежде чем воспользоваться любым сервисом с акциями и промокодами, узнайте, как давно он существует. А еще лучше – пользуйтесь только проверенными сервисами, с которыми вы уже знакомы. Условия там могут быть не такими привлекательными, зато и риска меньше.

# БУДЬТЕ БДИТЕЛЬНЫ!

**НЕ ПОДДАВАЙТЕСЬ НА ПРОВОКАЦИИ ИНТЕРНЕТ-МОШЕННИКОВ.**

# 4. НОВЫЕ СХЕМЫ МОШЕННИЧЕСТВА

## МОШЕННИКИ-КУКЛОВОДЫ: КАК И ЗАЧЕМ ОНИ ИЩУТ ПОСРЕДНИКОВ В ИНТЕРНЕТЕ

Все чаще в Сети можно встретить объявления о приеме на работу, обещающие высокий заработок за короткий срок, и с минимальными требованиями к кандидатам.

Будьте осторожны, возможно, за этими вакансиями стоят мошенники!

В таких объявлениях предлагается работа, связанная с переводом и обналичиванием денег, в основном "удаленка", без оформления документов, то есть неофициально. "Работодатели" используют такие слова, как "серьезный заработок за несколько часов", "трудоустройство без проверок и заполнения документов", "гарантия высокого дохода". Мошенники, которые публикуют данные вакансии, либо не указывают оклад, либо предлагают много денег за пару часов работы. В липовых объявлениях о приеме на работу не описаны конкретные профессиональные требования к соискателям, ни по уровню образования, ни по опыту работы, нет перечня их обязанностей, кроме как осуществление перевода денег и онлайн-взаимодействие с работодателем. Имейте в виду, что людей, которых принимают на такую работу, называют дропперами или дропами.

***Дроппер или дроп – это тот человек, который соглашается, чтобы его банковская карта стала "транзитной" для украденных мошенниками денег, либо он, сам того не зная, становится объектом мошенничества. В последнем случае дроп не всегда понимает, что его вовлекли в преступную схему, использовали в качестве посредника, поскольку аферисты умело замаскировали свои действия под "легальный бизнес".***



Дропа нанимают, чтобы он переводил незаконно полученные деньги между разными счетами. Это позволяет преступникам запутать свои следы и усложнить работу следствию. При этом мошеннические переводы могут совершаться в разных странах и от имени разных людей. За свою работу дроппер может получать процент от денежных средств, которые с его помощью перевели злоумышленники.

Следователи при расследовании случаев онлайн-мошенничества в первую очередь выходят на дропперов. Как правило, они становятся соучастниками преступления и могут получить соответствующее наказание, согласно ст. 190 Уголовного Кодекса РК "Мошенничество", вплоть до лишения свободы.

**СОВЕТ**

***Всегда помните про бесплатный сыр в мышеловке. Поэтому ни в коем случае не откликайтесь на подобного рода вакансии и не соглашайтесь на сомнительные предложения, если не хотите оказаться соучастником преступления.***

## ГДЕ ЕЩЕ ИСПОЛЬЗУЮТСЯ ДРОПЫ?

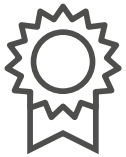
Дропперы нужны интернет-мошенникам в сфере продажи товаров, где применяется схема "товар по предоплате". Дроп назначается генеральным директором якобы официального интернет-магазина, который активно рекламируется в интернете. У такого магазина есть, казалось бы, подтверждающие документы, фишинговый сайт, отзывы покупателей. Мошенники после поступления заявки от клиентов просят предоплату за товар, люди им отправляют деньги, но взамен не получают ничего. А потом оказывается, что магазин закрылся, и вернуть деньги невозможно. При этом настоящих организаторов-аферистов найти не удается, а директор магазина может вообще не подозревать, что его попросту использовали.

**СОВЕТ**

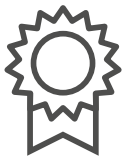
***Будьте осторожны, если вас просят отправить предоплату за товар. Нужно внимательно изучить информацию об интернет-магазине, его сайт, все ли разделы функционируют. Фишинговый сайт содержит множество грамматических и орфографических ошибок, на нем могут быть размещены фейковые отзывы от "покупателей". К примеру, они могут быть написаны "под копирку", либо имена пользователей и их фотографии будут весьма странными. Почитайте о данном сайте в СМИ, в соцсетях.***



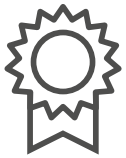
# ЗНАЙТЕ, ЧТО НАСТОЯЩИЕ ПРОДАВЦЫ ДОЛЖНЫ:



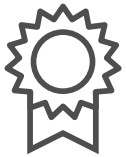
размещать ссылки на интернет-ресурсы (электронная торговая площадка, интернет-магазин), с содержанием сведений об основных потребительских свойствах товара, наименовании продавца, его юридического адреса и абонентского номера, зарегистрированного у оператора сотовой связи Казахстана;



предоставить перед заключением договора купли-продажи потребителю на казахском и (или) русском языках информацию о товаре, его стоимости, процедуре оплаты, условиях и стоимости доставки, гарантийном сроке (при его наличии);



при продаже товара по образцу и (или) описанию передать потребителю товар, который соответствует образцу и (или) описанию;



иметь в наличии документы, подтверждающие право собственности продавца на товары, исключением являются товары собственного производства.

Мошенники часто используют дропов в качестве курьеров. Они размещают вакансию на сайтах о трудоустройстве. Когда нужный кандидат находится, то аферисты просят его онлайн отправить сканы документа, удостоверяющего личность, чтобы якобы "пройти проверку службы безопасности", а иногда и скан платежной карты – якобы для зачисления заработной платы А потом мошенники не перезванивают, пропадают и используют документы и карточку своей жертвы в своих корыстных целях.

**СОВЕТ**

***Никогда не высылайте свои документы и другие личные данные, в том числе реквизиты платежных карточек, пин-коды, пароли от личных аккаунтов, посторонним лицам. Серьезные организации назначают встречу, собеседование и не запрашивают ваши персональные и платежные данные. После заключения трудового договора работодатели тем более не запрашивают секретные коды и пароли (CVV, CVC-коды, SMS и другое). Эти данные не стоит раскрывать никому, кто настойчиво просит их переслать.***

Дропперами чаще становятся те граждане, которые верят, что могут быстро и легко заработать, кто остро нуждается в деньгах и соглашается на любую работу. Мошенники это прекрасно понимают и пользуются этим. Поэтому чаще всего в качестве кандидатов они рассматривают и пытаются заманить в свои сети студентов, безработных, представителей маломобильных групп, в том числе пожилых граждан.

Дропперы, участвующие в мошеннических схемах, несут правовую ответственность по законодательству Республики Казахстан. И, прежде чем соглашаться на якобы выгодные предложения, которые могут показаться вам сомнительными, стоит сто раз подумать.



# МОШЕННИЧЕСТВО С QR-КОДАМИ: КАК СЕБЯ ОБЕЗОПАСИТЬ

Одним из распространенных способов оплаты являются QR-платежи посредством мобильных устройств. Однако всегда ли безопасно сканировать QR-коды?

***Quick response code (QR-код)*** – код быстрого реагирования – двумерный штрих-код, предназначенный для считывания закодированной информации. QR-код может считываться с помощью устройств обработки изображений, например, камеры или специальной функции.

Для осуществления QR-платежей пользователю необходимо отсканировать QR-код продавца с помощью смартфона, который привязан к платежной карточке или электронному кошелку. QR-сервисы могут использоваться как для платежей в торговых точках, так и в интернете. Важно отметить, что при QR-платежах продавцу не нужен POS-терминал. При сканировании QR-кода происходит прямой перевод средств, и продавец моментально получает уведомление о поступлении денежных средств. Это значительно ускоряет и упрощает процесс оплаты за товары и услуги.

***Хотя QR-коды существуют уже более 25 лет, их использование в повседневной жизни резко возросло в последние несколько лет. Наше доверие и частое использование QR-кодов не обошло стороной и мошенников. На какие ухищрения идут злоумышленники для получения доступа к вашим персональным данным посредством QR-кода?***

## КАК РАБОТАЕТ QR-МОШЕННИЧЕСТВО

Технически не существует такого понятия как "поддельный" QR-код. Коды сами по себе не опасны — проблема может заключаться в том, кем и как они используются. Создать QR-код очень легко, используя ряд бесплатных онлайн-генераторов, который при сканировании автоматически перенаправляет на вшитый URL-адрес. Используя тот факт, что человеческий глаз не может "прочитать" QR-код, мошенники легко могут заменить настоящий код своим собственным. Эти "поддельные" QR-коды могут перенаправить вас на вредоносные веб-сайты, предназначенные для кражи вашей конфиденциальной информации. Разберем на примерах, что может скрываться в мошеннических QR-кодах.


## *ПРИМЕР* №1

***Мошенничество с QR-кодом при бесконтактных платежах.***

Одним из наиболее распространенных способов применения QR-кодов является оплата за товары и услуги, к примеру food court или парковку. Однако перед тем, как совершить платеж QR-кодом внимательно проверьте наименование и защищённость сайта, он должен начинается с **https** и иметь символ закрытого замка. Встречаются случаи, когда ничего не подозревающие граждане сканировали QR-код в общественных местах и попадали на фишинговые веб-сайты.



## *ПРИМЕР* №2

***Поддельные QR-коды, отправленные на электронную почту.***

При совершении онлайн-покупок на вашу электронную почту может поступить сообщение о "неудачном платеже". Для того чтобы завершить транзакцию вам необходимо отсканировать QR-код. Такие сообщения могут рассылать мошенники, если вы приобретаете товары на сайтах, на которые совершены хакерские атаки. Если вы считаете, что онлайн-покупка не состоялась, войдите в свою учетную запись непосредственно на веб-сайте компании, а не с помощью QR-кода.

## *ПРИМЕР* №3

***QR-коды на неожиданных посылках.***

Мошенникам могут сыграть на вашем чувстве любопытства. Один из самых простых способов сделать это – отправить товар от интернет-магазина, который вы не заказывали. Внутри или на упаковке вы увидите QR-код с "инструкцией" о том, как его вернуть (или узнать больше информации о вашем заказе). Если вы отсканируете код, то он автоматически перенаправит вас на фишинговый веб-сайт, который получит доступ к вашей личной информаций и даже реквизиты банковской карты. Другая версия этого мошенничества – письменное уведомление с QR-кодом на вашей двери о "пропущенной посылке". Когда вы отсканируете QR-код, то вас попросят ввести личные данные или оплатить дополнительную стоимость доставки. Если вы получили посылку, которую не ожидали, то лучше сообщить об этом службе доставки напрямую.

## *ПРИМЕР* №4

***QR-коды, отправленные через социальные сети (взломанные аккаунты).***

Мошенники могут отправить вам поддельные QR-коды через взломанные учетные записи социальных сетей, содержащие сообщение, к примеру от вашего друга: "Посмотри на эту твою фотографию, которую я только что нашел!" Поскольку вы думаете, что сообщение от "друга", вы, скорее всего, отсканируете его. Захват учетных записей в социальных сетях распространен на всех платформах. Если учетная запись, на которую вы подписаны, отправляет вам странное сообщение, содержащее QR-код, свяжитесь с человеком напрямую (за пределами этой платформы), чтобы убедиться, что его учетная запись не взломана.

## *ПРИМЕР* №5

***Мошенничество с криптовалютным QR-кодом.***

Из всех типов мошенничества с QR-кодом этот вид связан с одним из самых больших финансовых потерь. Мошенники от лица псевдоинвесткомпаний могут предложить инвестировать в криптовалюты. Они высылают вам QR-код, который откроет процессор платежей, позволяющий конвертировать ваши деньги в биткойны, эфириум и другие криптовалюты. Но как только вы делаете перевод, мошенники либо исчезают, либо требуют, чтобы вы заплатили больше.



## ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ВВЕЛИ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ В ПОДДЕЛЬНЫЙ QR-КОД?

1. ***Позвоните в свой банк и заблокируйте все счета, а также сообщите в службу безопасности банка о возможном мошенничестве.***

2. ***Измените все пароли во всех своих аккаунтах. Используйте безопасные пароли длиной не менее восьми символов, включающие прописные и строчные буквы, символы и цифры. Установите антивирус, который защитит гаджет от вредоносных программ.***

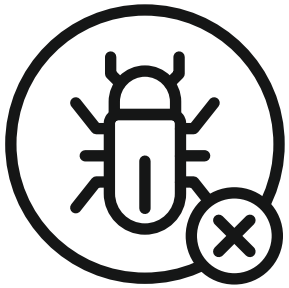
## ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОТСКАНИРОВАЛИ QR-КОД, КОТОРЫЙ ЗАГРУЗИЛ ВРЕДОНОСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА ВАШЕ УСТРОЙСТВО?

1. *Отключитесь от сети Wi-Fi или сотовой сети. Отключите любое сетевое соединение, как только поймете, что могли загрузить вредоносное ПО. Без подключения меньше шансов, что вредоносное ПО сможет отправить вашу конфиденциальную информацию хакеру.*

2. *Сделайте резервную копию важных файлов. Если ваше устройство взломают, мошенники могут украсть конфиденциальные документы и фотографии или даже зашифровать ваш диск и заставить вас заплатить выкуп. Сделайте резервную копию ваших файлов на внешнем диске для дополнительной безопасности.*

3. *Срочно меняйте пароли. Вредоносное ПО может предоставить мошенникам доступ к вашим онлайн-аккаунтам — социальным сетям, банковским операциям, криптовалюте, магазинам и многому другому. Обновите свои пароли, включите 2FA и начните использовать менеджер паролей.*

4. *Просканируйте свое устройство на наличие вредоносных программ. Антивирусное программное обеспечение обладает возможностями защиты от вредоносных программ и может предупредить вас о любых угрозах кибербезопасности.*






## СОБЛЮДАЙТЕ КИБЕР-ГИГИЕНУ

1. Никогда не сообщайте никому пароли, коды или иные конфиденциальные данные, используемые для подтверждения платежей. Современные системы безопасности создаются таким образом, чтобы пароли и коды не передавались другим людям.

2. Проверяйте URL-адреса. Особенно ссылки, полученные от незнакомых отправителей. Зачастую злоумышленники используют похожие по написанию домены.

3. Проверяйте наличие префикса **https** на сайтах, где требуется ввести конфиденциальную информацию, например, пароли.

4. Большинство современных браузеров содержат встроенные механизмы противодействия массовым фишинг-атакам. Необходимо обращать внимание на сообщения браузера об угрозах и потенциально опасном содержимом сайтов.

5. Если вы сомневаетесь, является ли сайт или страница организации фейковой, свяжитесь с данной организацией и уточните информацию, особенно, если вы собираетесь совершить платежи в системе интернет-банкинга своего банка. Лучше позвоните в банк и уточните информацию. И помните, что банковские менеджеры не звонят клиенту первыми, поэтому если вам позвонили и запросили код из SMS, чтобы заблокировать непонятные транзакции на вашем счету, завершите телефонный разговор и обратитесь в обслуживающий банк.

6. Если вы зарегистрировались на подозрительном сайте, то для защиты своих персональных данных следует сменить электронную почту.



# ТОЧЕЧНЫЕ ФИНАНСОВЫЕ АТАКИ:

## КАК УБЕРЕЧЬСЯ ОТ МОШЕННИКОВ

Очередные способы финансового мошенничества связаны с перехватом SMS-сообщений от банка. Мы расскажем подробнее, как работают эти схемы, и как можно обезопасить себя и свою карту от финансовых мошенников.


**SIM-свопинг (подмена SIM-карты)** стал широко известен в мире после серии крупных краж криптовалют. Но с помощью подмены SIM-карт можно также выкрасть деньги с банковских счетов или обналичить средства с платежной карты, если они привязаны к номеру телефона. Ведь подтверждение финансовых операций, будь то перевод денег с карты на карту или оплата товаров и услуг в системе онлайн-банкинга, с помощью SMS-сообщений – дело привычное, можно сказать, рутинное.

SIM-свопинг или подмена SIM-карты – это схема, при которой злоумышленники узнают телефонный номер жертвы и обращаются к мобильному оператору, выдавая себя за нее, с просьбой повторно выпустить SIM-карту на себя. При успешной атаке мошенники получают полный контроль над привязанным к телефонному номеру аккаунтом.

Следует знать, что SIM-свопинг – это точечная финансовая атака и довольно трудоемкая, соответственно мошенники используют ее применительно к определенному клиенту, у которого наверняка есть крупная сумма на карте.

К сожалению, вернуть деньги, украденные посредством такой мошеннической схемы, весьма затруднительно. Если вы стали жертвой SIM-свопинга, то следует непременно обратиться с заявлением в правоохранительные органы, а также обязательно известить об инциденте свой банк, оператора мобильной связи и Агентство РК по регулированию и развитию финансового рынка.

Подмена телефонного номера – еще один способ мошенничества. Выглядит он так: вам звонят с знакомого номера (банка или иной финансовой организации) и просят сообщить, к примеру, реквизиты платежной карты или назвать код из SMS-сообщения, который был отправлен на ваш номер. Это делается якобы в целях вашей безопасности, например, из-за подозрительной активности на ваших счетах. Передав важную информацию злоумышленникам, вы тем самым рискуете своими средствами на карте и счетах.

Если мошенник владеет достаточной информацией о вас, он может от вашего имени покупать товары и услуги, открывать новые счета, переводить деньги или подавать заявки на получение кредитов.

Современные технологии позволяют "подделать" любой номер, причем сами мошенники могут находиться на другом конце планеты. Соответственно, компенсировать убытки будет невозможно. В отличие от схемы с SIM–свопингом, здесь работает принцип "ваша безопасность – в ваших же руках", то есть безопасность ваших средств зависит от вашей осторожности и бдительности. Не следует никому сообщать конфиденциальную информацию. Правильно будет – закончить разговор, повесив трубку, и позвонить в обслуживающий банк, чтобы уточнить информацию. Желательно также посетить ближайшее отделение банка и написать заявление о попытке мошенничества.

Помните, что в финансовых организациях существует регламент действий банковских сотрудников, в соответствии с которым они никогда не звонят первыми клиенту с требованием предоставить данные по карте, либо полученные SMS. Любое общение по данным вопросам инициируется исключительно клиентом.



# ФАЛЬШИВЫЕ ПЕРЕВОДЫ И ДРУГИЕ МЕТОДЫ СОЦИАЛЬНОГО МОШЕННИЧЕСТВА


**Вам приходит SMS.**

Есть два основных метода, с помощью которых злоумышленники пытаются выманить средства у граждан. Первый более технологичный и рассчитан на невнимательность потенциальной жертвы и психологическое давление. Вам приходит SMS о зачислении определенной суммы средств на вашу банковскую карту. Сумма обычно не слишком большая, но и не маленькая. И пока вы задумываетесь, откуда могли поступить деньги, вам звонит некий человек и сообщает об ошибочном переводе. Он или она слезно просят сделать обратный перевод, а еще лучше, если под рукой есть терминал, а у вас наличные, провести оплату какой-нибудь услуги или банально "положить денег на телефон". Мошенники рассказывают множество подробностей о себе и последствиях сделанной ошибки. У кого-то это якобы последние деньги, кто-то якобы может потерять работу, и т. д. Это сигнал к тому, что вас попросту пытаются отвлечь. На самом деле, никакого перевода вам не поступало. А SMS пришло с номера, очень похожего, но все же отличающегося от номера вашего банкинга. Кроме того, всегда можно проверить, действительно ли на ваш счет были перечисления в личном кабинете и истории переводов.

## ЕСЛИ ПЕРЕВОД РЕАЛЕН?

Второй метод более изощрен. Допустим, деньги на ваш счет действительно поступили. Сценарий может быть примерно таким же – якобы ошибочный перевод и просьба вернуть средства прямо сейчас. Мошенники иногда даже предлагают оставить небольшую часть средств у себя – "за беспокойство". На самом деле злоумышленники могли указать ваш счет для получения оплаты якобы за продажу товара на торговой площадке. Тогда в случае, если вы поддадитесь уговорам и

сделаете перевод, вы останетесь не только без денег, но и наживете себе дополнительных проблем. Ведь потенциальный покупатель, не получив товар, может обратиться в правоохранительные органы. А вы, как получатель денег, окажетесь первым подозреваемым. Зацепкой здесь может послужить тот факт, что средства могли поступить с одного счета, а просят сделать перевод на другой. "Жена перепутала", – сетует мошенник.

## ПЕРЕВЕДИТЕ МНЕ КРЕДИТ!

Однако видеть, от кого именно сделан перевод можно не всегда. Ведь это может быть "карта другого банка" или даже счет какой-нибудь организации. Здесь нужно насторожиться вдвойне. Одна из главных мошеннических схем – оформление кредитов на третьих лиц. Обычно это происходит, когда злоумышленники смогли заполучить доступ к вашим персональным данным. Тогда в случае, если вы переведете им средства, вы останетесь должны эту сумму, да еще и с процентами, а главное – неизвестно кому. О таких кредитах пострадавшие узнают обычно к концу срока оплаты или еще хуже – от коллекторов. Ведь для подтверждения выдачи займа мошенник указал ваши данные, но свой номер телефона, скорее всего, уже не работающий. Поэтому никаких звонков с напоминанием вам, конечно же, не поступало. Фиктивный кредит, конечно же, можно оспорить через суд, но это займет Ваше время.

## ОТ ДЕНЕГ ОТКАЗЫВАЮСЬ!

Главный способ защиты от фейковых переводов – вести все операции только в официальном поле и через свой банк. Вам необходимо сразу сообщить по телефону горячей линии, что перевод, поступивший вам на карту, ошибочный и использовать эти средства вы не намерены. Мошенникам на все уговоры следует отказывать и отправлять опять же – в банк. В таких случаях они могут резко изменить линию поведения и начать, например, угрожать судом. Не переживайте, если вы все сделали официально, вам ничего не грозит. Как можно скорее стоит зайти в отделение банка и написать официальное заявление об отмене перевода. Обязательно получите копию заявления с входящим номером, ведь это – ваш главный документ для защиты. Теперь вам остается только оставить полученную сумму на счету, то есть, ни в коем случае ее не тратить и ждать обратной транзакции.



"ГОРЯЧАЯ" ТЕМА:

# 5. КАК УБЕРЕЧЬ СВОИХ ДЕТЕЙ ОТ МОШЕННИКОВ

***В какие онлайн-ловушки могут попасть дети и как обезопасить их от кибермошенников – разберемся в этих вопросах.***

# ИГРОВЫЕ ПРИЛОЖЕНИЯ С ВРЕДОНОСНЫМ КОДОМ

Большинство финансовых мошенничеств, которые могут коснуться современных детей, обычно происходит при покупке мобильных или компьютерных игр. Во многих онлайн-играх пользователям предлагается приобрести снаряжение, игровые бонусы для "прокачки" до максимального уровня или разблокировать какие-то новые локации. Довольно заманчиво предложение купить те или иные игровые предметы со скидкой, либо приобрести платную игру без рекламы по заниженной стоимости. Однако не все эти покупки безопасны. Злоумышленники таким образом могут распространять вредоносные приложения. И вместо "скидочной" игры от неизвестного источника можно "впустить" в гаджет вирусную программу, которая будет собирать персональные данные и сведения о банковских картах и счетах, если ребенок скачивает приложения на телефоне родителей, где зачастую установлено банковское мобильное приложение. В итоге, мошенники, выведав эту конфиденциальную информацию, без труда могут обнулить ваш счет. Поэтому лучше не давать детям играть на своем телефоне, если к нему привязаны банковские карточки, особенно зарплатная карта, или хранится другая важная информация. Также стоит установить ограничения на покупки с телефонов и регулярно проверять платные подписки, которые маленький ребенок может оформить случайно.



Детям постарше, которым родители оформили свою карту и имеющим собственный гаджет, надо объяснить, какие могут быть последствия, если скачивать сомнительные приложения. В случае, если совместно с ребенком вы все же решили совершить онлайн-покупку, то лучше для этих целей использовать виртуальную карточку, на которую следует закинуть только ту сумму, которую собираетесь потратить.

**СОВЕТ:** ***лучше всего совершать все онлайн-покупки с помощью отдельной платежной карты, не привязанной к зарплатной, и только на проверенных сайтах, скачивать приложения из официальных магазинов.***

# "СБОРЩИК" ИНФОРМАЦИИ

Существуют "умные" приложения, которые могут собирать геоданные и иные персональные сведения и таким образом следить за вашими действиями. Опять-таки дети, сами того не осознавая, могут скачать такие приложения на свой или родительский телефон. Эти "сборщики" конфиденциальной информации позволяют с легкостью выяснить, где вы живете, работаете, где учится ваш ребенок, где проводите больше времени, отдыхаете, что обычно покупаете онлайн и многое другое. Таким образом, злоумышленникам не составит труда узнать ваши интересы и увлечения ваших детей. А некоторые приложения еще и предоставляют доступ кибермошенникам в почтовые сервисы, социальные сети, что очень опасно. Поэтому будьте бдительны перед установкой различных приложений на свой гаджет.

Кстати, узнать, что приложение отслеживает местоположение не так уж и трудно. Проверить это можно в настройках телефона. В IOS нужно зайти в раздел "Настройки", далее "Конфиденциальность" и в "Службы геолокации". В Android нужно открыть "Настройки" и далее зайти в разделы "Местоположение" и "Доступ приложений к геоданным". Лучше отключить функцию геолокации сразу для всех приложений, а сомнительные и вовсе удалить.

**СОВЕТ:** ***установите на свой гаджет и гаджет ребенка антивирусные программы и регулярно их обновляйте. Обязательно перед установкой приложений и программ проверяйте их на вирусы. Отключите сведения о местоположении на фотографиях, в приложениях и при публикации постов в социальных сетях.***

## ФАЛЬШИВЫЙ ПРОФИЛЬ В ИНТЕРНЕТЕ

Мошенники зачастую маскируют свой профиль под аккаунт ребенка в социальных сетях, на форумах или в онлайн-играх. Вашим детям может казаться, что они общаются со сверстником, а на самом деле это может быть взрослый человек или мошенник. Нередки случаи, когда такие виртуальные "друзья" могут подговорить ребенка сфотографировать и отправить им платежную карту родителей, продиктовать SMS-код, который придет на телефон или скачать вредоносное приложение.

**СОВЕТ:** ***Наладьте диалог со своим ребенком, беседуйте с ним о его виртуальных друзьях, как если бы речь шла о друзьях в реальной жизни. Расскажите ему, что все, что он публикует в интернете, является общедоступным и сохраняется во Всемирной паутине, где любой желающий может воспользоваться этими данными. Объясните ребенку, почему нельзя доверять незнакомым людям, особенно в интернете, и какие данные нельзя раскрывать.***



## ПРАВИЛА БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ, КОТОРЫЕ ДОЛЖЕН ЗНАТЬ КАЖДЫЙ РОДИТЕЛЬ!

- Ограничьте время, проводимое в интернете.
- Используйте антивирус, как на компьютере, так и на телефонах.
- Не запускайте неизвестные вложенные файлы, присланные на электронную почту и мессенджеры.
- Объясните ребенку, почему нельзя передавать свой пароль никому, за исключением родителей.
- Фильтруйте контент. Для этого используйте бесплатные рекурсивные DNS-сервисы (например: "OpenDNS", "Quad9", "Yandex").

# 6. ЧТО НУЖНО ЗНАТЬ ПРО БЕЗОПАСНЫЕ КРЕДИТЫ

## НЕ ОФОРМЛЯЙТЕ ЗАЙМЫ В СОМНИТЕЛЬНЫХ ОРГАНИЗАЦИЯХ!

*Нашли компанию, оформляющую займы под залог автомобилей, бытовой техники, ноутбуков, сотовых телефонов? Какую информацию о ней надо проверить в первую очередь?*



Рекомендуем для начала ознакомиться с Реестром микрофинансовых организаций, прошедших учетную регистрацию. Данный Реестр размещен на официальном сайте Агентства РК по регулированию и развитию финансового рынка **www.finreg.kz** в рубрике "Реестр разрешений и уведомлений".

Если компании нет в списке, значит, ее деятельность не подлежит регулированию со стороны уполномоченного органа. Доверите ли вы такой компании свои средства?

Также проанализируйте информацию, размещенную на сайте финансовой организации, клиентом которой вы хотите стать. Если организация, к примеру, именует себя ломбардом, но при этом указывает на своем сайте, что занимается открытием вкладов, это должно вас насторожить. Прием депозитов относится к банковским операциям, осуществлять которые могут банки второго уровня, имеющие соответствующую лицензию финрегулятора, а также Национальный оператор почты без лицензии уполномоченного органа в лице Агентства РК по регулированию и развитию финансового рынка.

# 7. КАК НЕ ЗАПЛАТИТЬ ПО ЧУЖОМУ КРЕДИТУ?

***Зачастую граждане даже не подозревают, что являются должниками, до тех пор, пока к ним не обращаются из службы взыскания банков или коллекторского агентства. Таким образом, вопросы незаконного оформления займов на третьих лиц в последнее время приобретают особую актуальность.***

## КАК УЗНАТЬ, ОФОРМЛЕН ЛИ НА ВАС КРЕДИТ, КОТОРЫЙ ВЫ НЕ БРАЛИ?

Выявить факт незаконного оформления кредита на ваше имя своевременно позволит кредитная история. Отслеживание своей кредитной истории – это своего рода "страховка" от мошенников. В базе данных кредитных бюро есть сведения обо всех заемщиках каждого банка и кредитной организации по всему Казахстану. То есть, если вы хоть раз брали кредит, то эта информация, в том числе по просрочкам, если они были, будет отражена в этой базе данных. Поэтому рекомендуем регулярно проверять свою кредитную историю через любые доступные источники:

- в Государственном кредитном бюро – **mkb.kz**
- в Первом кредитном бюро – **1cb.kz**
- на сайте государственных услуг – **egov.kz**
- в центрах обслуживания населения

Следует помнить, что кредитный отчет предоставляется бесплатно только один раз в год. Кредитные бюро хранят кредитную историю в течение как минимум десяти лет с момента, когда была получена последняя информация о кредите. Помните, что информация в персональном кредитном отчете является конфиденциальной. **Ее нельзя раскрывать третьим лицам!**

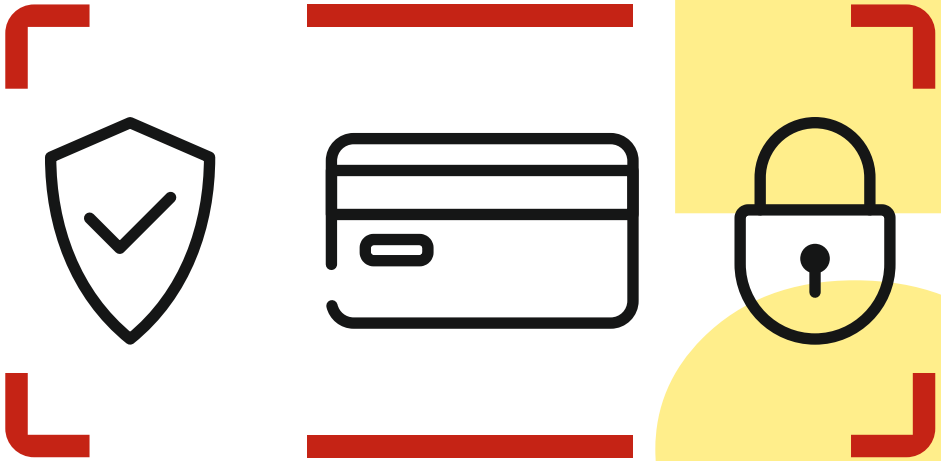
## ЧТО ДЕЛАТЬ, ЕСЛИ НА ВАС ОФОРМИЛИ КРЕДИТ БЕЗ ВАШЕГО ВЕДОМА?

В первую очередь, необходимо узнать наименование кредитной организации, в которой оформлен заем. Проверить, находится ли данная организация в периметре регулирования Агентства РК по регулированию и развитию финансового рынка, можно на сайте финансового регулятора **www.finreg.kz** в разделе "Реестр разрешений и уведомлений". Выяснив, в какой кредитной организации мошенники получили заем на ваше имя, вам необходимо написать заявление в данную организацию, подробно указав в нем всю имеющуюся информацию. В случае утери платежной карты или документа, удостоверяющего личность, необходимо приложить подтверждающую справку. Обязательно потребуйте проведения внутреннего служебного расследования. Ваше заявление должны зарегистрировать, регистрационный номер с датой принятия заявления необходимо поставить и на копии заявления, которую вы оставляете себе. Кроме того, кредитная организация должна предоставить вам копии договора, приложений к нему и документов, удостоверяющих личность.

Следует отметить, что воспользоваться таким способом могут не только незнакомые люди, но и близкие родственники, подруги, друзья, знакомые – люди, кому вы доверили когда-то свои документы, реквизиты карты или счета.

## ОТВЕТСТВЕННОСТЬ ЗА ПОЛУЧЕННЫЙ КРЕДИТ.

Если работник банка или микрофинансовой организации просит Вас получить кредит для него или передать часть полученного кредита, уверяя, что оплачивать будет самостоятельно, то следует понимать, что ответственность за возврат кредита остаётся за клиентом до полного погашения всего кредита, независимо от того кому и каким образом переданы денежные средства.



# 8. ПОЧЕМУ НЕ СТОИТ ДОВЕРЯТЬ “КРЕДИТНЫМ ПОСРЕДНИКАМ”

В Казахстане появились “кредитные помогайки”, предлагающие посреднические услуги в оформлении займов, обналичивании товарных кредитов. Их схемы обмана основываются на доверии граждан, которые добровольно передают мошенникам свои персональные данные. При этом взаимодействуют злоумышленники со своими жертвами исключительно онлайн, чтобы вовремя замести свои следы.

“У вас плохая кредитная история? Поможем быстро оформить кредит от 200 тыс. до 3 млн тенге, без залога и предоплаты, высокий процент одобрения.” “Оформим для вас микрокредит на любую сумму и на любые цели. Гарантия – 100%.” “Вам срочно нужны деньги? Оформите товар в рассрочку, а мы его выкупим по хорошей цене.” “Устали отдавать все деньги кредиторам? Поможем удалить ваш кредит из базы банка и МФО и почистим вашу кредитную историю.”

Объявления с таким содержанием “помогайки” размещают в социальных сетях, в основном в Instagram, создавая фейковые аккаунты-однодневки.

Взаимодействие мошенников с пользователями, которые откликнулись на объявления, происходит через мессенджеры. При этом злоумышленники предпочитают вести переписку посредством WhatsApp, в котором имеется режим исчезающих сообщений, и действуют по одной из двух схем. Рассмотрим их подробнее.



## ПЕРВАЯ СХЕМА: ОФОРМЛЕНИЕ КРЕДИТА НАЛИЧНЫМИ

Якобы в целях оформления займа интернет-мошенники уточняют у потенциальной жертвы необходимую сумму кредита и личные сведения: данные документа, удостоверяющего личность, полные реквизиты платежных карточек, номера счетов и так далее. Целью мошенников является оформление на пострадавшего кредитов, существенно превышающих потребности заемщика. Злоумышленников особенно интересует наличие у граждан личных кабинетов на популярных ресурсах онлайн-кредитования. По их словам, данная информация необходима для того, чтобы оформить выгодный кредит, который кредитные организации стопроцентно одобрят.

На самом деле мошенники делают все возможное, чтобы получить доступ к личным кабинетам граждан со своих устройств. Для восстановления пароля они запрашивают SMS-код у доверчивых “клиентов”, объясняя это тем, что необходимо оформить и подать заявку на микрокредит. “Взломав” личный кабинет, мошенники с легкостью могут изменить мобильный номер, привязанный к онлайн-сервису, и указывают свой номер, зарегистрированный на подставных лиц. Далее они начинают подавать от имени жертвы заявки в различные МФО на получение онлайн-займов.

В случае одобрения микрокредита, мошенники просят заемщиков перевести всю сумму займа или ее часть на баланс указанного ими номера телефона для якобы досрочного закрытия полученного займа и направления новой заявки. Они убеждают заемщиков, что так надо обязательно сделать, чтобы система скоринга кредитной организации считала их "лояльными клиентами" и в дальнейшем позволила взять сумму в разы больше.

Либо же мошенники обманным путем получают персональные и платежные данные заемщиков, и, соответственно, доступ к их онлайн-банкингу, к примеру, через приложение AnyDesk. Затем они переводят все средства со счетов граждан на счета третьих лиц – дропперов или на баланс подставных номеров телефона, затем выводят эти деньги и удаляют переписку.

Дропперов мошенники обычно "нанимают", чтобы они переводили незаконно полученные деньги между разными счетами. Это позволяет преступникам запутать свои следы и усложнить работу следствию. При этом мошеннические переводы могут совершаться в разных странах и от имени разных людей. За свою работу дроппер может получать процент от денежных средств, которые с его помощью перевели злоумышленники. А заемщик остается у разбитого корыта – без денег и без доказательств того, что он доверился мошенникам.



## СХЕМА МОШЕННИЧЕСКИХ ДЕЙСТВИЙ ПРИ ОФОРМЛЕНИИ ДЕНЕЖНЫХ МИКРОКРЕДИТОВ

1. Поиск жертв среди откликнувшихся граждан на объявления о помощи в оформлении займов, размещенных на созданных мошенниками аккаунтах в Instagram.

2. Переговоры с гражданами посредством мессенджеров и соцсетей с целью получения конфиденциальной информации (данный удостоверения личности, полные реквизиты карточек, номера счетов и т. п.).

3. Получение доступа с мобильного телефона, не принадлежащего заемщику, к его личному кабинету с использованием персональных данных жертвы и функции "восстановить пароль". Информация о новом пароле или SMS-код для его восстановления запрашивались у жертв под предлогом необходимости оформления заявки на микрокредит.

4. Смена номера телефона в личном кабинете жертвы на имеющиеся в распоряжении мошенников номера телефонов, зарегистрированных на подставных лиц. И подача с мошеннических номеров заявок на получение онлайн-займов от имени потерпевших.

5. В случае получения займа злоумышленники связываются с жертвой с просьбой вернуть всю сумму займа или ее часть посредством пополнения баланса указанного мошенниками номера телефона для якобы досрочного закрытия полученного займа и направления новой заявки для получения большей суммы.

6. Вывод денежных средств с баланса телефона посредством цифровых карт, к примеру, "Simply", на банковский карты третьих лиц и их последующее обналичивание.

## ВТОРАЯ СХЕМА: ОФОРМЛЕНИЕ ТОВАРНЫХ КРЕДИТОВ

Получив персональные данные заемщиков, которые откликнулись на объявления "кредитных посредников", мошенники со своих мобильных телефонов и с использованием номеров, зарегистрированных на подставных лиц, на сайтах продавцов электроники выбирают товар и с помощью заемщика оформляют его в кредит или рассрочку. При этом злоумышленники указывают свои номера, куда приходят SMS-коды для рассмотрения заявки. Изобретательные мошенники также указывают способом доставки либо самовывоз из магазина, либо доставку курьером по указанным ими адресам.

Получив одобрение по кредиту, злоумышленники сообщают заемщикам, что у них не получилось оформить товарный кредит, или же они оформляют несколько товаров, а своему "клиенту" передают только один.

При выдаче товаров мошенникам поступает SMS-код, который они сообщают работнику магазина или курьеру. Получив товар, мошенники с помощью подставных лиц стараются его побыстрее реализовать, а на связь с заемщиком, разумеется, уже не выходят.



## СХЕМА МОШЕННИЧЕСКИХ ДЕЙСТВИЙ ПРИ ОФОРМЛЕНИИ ТОВАРНЫХ КРЕДИТОВ

1. Поиск жертв среди откликнувшихся граждан на объявления о помощи в оформлении займов, размещенных на созданных мошенниками аккаунтах в Instagram.

2. Переговоры с гражданами посредством мессенджеров и соцсетей с целью получения конфиденциальной информации (данный удостоверения личности, полные реквизиты карточек, номера счетов и т. п.).

3. Подача мошенниками заявки с мобильных телефонов, не принадлежащих заемщикам, и с использованием номеров, зарегистрированных на подставных лиц, на сайтах продавцов электроники на покупку товара в рассрочку. В качестве способа доставки способа доставки злоумышленники указывают самовывоз из магазина или доставку курьером по указанным ими адресам.

4. Получив одобрение по кредиту, мошенники сообщают заемшикам, что у них не получилось оформить товарный кредит, или же они оформляют несколько товаров, а жертве передают только один.

5. Мошенники при помощи третьих лиц получают товар в магазине или через курьера.

6. Реализация злоумышленниками товаров, приобретенных за счет займов, оформленных на пострадавших.

# ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ?

Необходимо незамедлительно обратиться в правоохранительные органы, а также в банк, чтобы заблокировать свои карточки. Карточки банк заблокирует и перевыпустит новые.

Обязательно поменяйте пароли от личного кабинета в банковском приложении на онлайн-сервисах по оформлению микрокредитов.

Раз в квартал проверяйте свою кредитную историю, чтобы убедиться, что мошенники не оформили на ваше имя фиктивный заем. Персональный кредитный отчет можно получить в кредитных бюро (Государственное кредитное бюро или Первое кредитное бюро), в ЦОНах или на сайте **egov.kz**. По закону один раз в календарный год персональный кредитный отчет можно запросить бесплатно.

# СОБЛЮДАЙТЕ ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ, ЧТОБЫ УБЕРЕЧЬ СВОИ ДАННЫЕ ОТ ФИНАНСОВЫХ МОШЕННИКОВ

Не верьте посредникам, которые предлагают вам оформить банковские займы или микрокредиты на выгодных условиях, не давайте денежного вознаграждения за оформление кредита. Это мошенники.

Обращайтесь за займами и микрокредитами напрямую в банки или микрофинансовые организации. Но помните, что любой кредит – это большая ответственность!

Не передавайте посторонним лицам через WhatsApp, Telegram, Viber и другие мессенджеры информацию о себе и своей карте: пароли, логины, коды и другие личные данные (ИИН, номер удостоверения личности или паспорта, реквизиты платежной карты: трехзначный код с обратной стороны карты (CVV/CVC-код), ее номер, срок действия и т. д.). Не публикуйте в социальных сетях фотографии своих документов, удостоверяющих личность, и платежных карточек.

Если с вами связался (по телефону или онлайн) якобы менеджер банка или МФО и сообщил о мошеннических атаках на ваш счет, попросил перевести деньги на "безопасный" счет, оформить "зеркальный" кредит или снять средства через банкомат, завершите разговор. Позвоните в call-центр кредитной организации, чтобы перепроверить информацию.

***Запомните: представители финансовых организаций не звонят первыми и не пишут через мессенджеры, чтобы выведать ваши персональные данные, и тем более не предлагают посреднические услуги.***

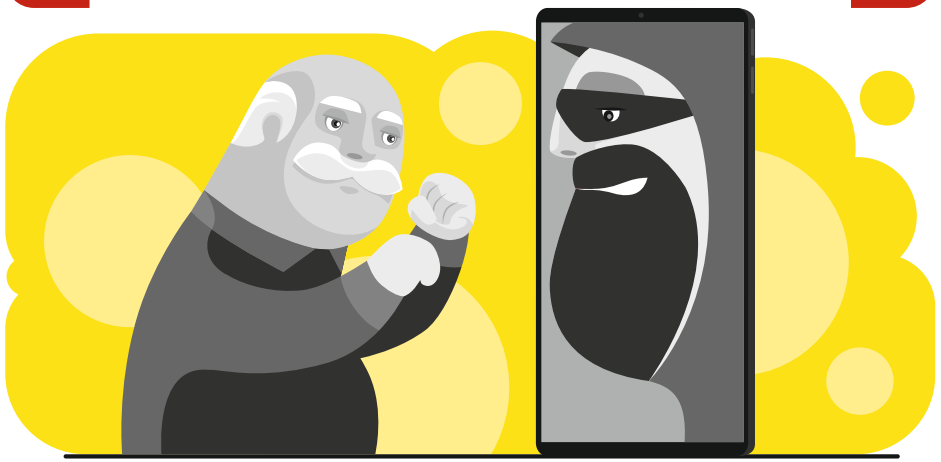


Не скачивайте по инструкции незнакомых людей приложения, которые могут быть вирусными, шпионскими или позволяют третьим лицам дистанционно управлять вашим устройством (например, AnyDesk или TeamViewer).

Не переходите по фишинговым ссылкам. Прежде чем пройти регистрацию на подозрительных сайтах, проверьте их адрес, который должен начинаться с **https**.

При открытии счета или карты подключите услугу SMS- или push-уведомлений об операциях. Используйте сложные пароли в своем мобильном банковском приложении, а также для почты и аккаунтов в соцсетях. Пароли должны быть разными. Регулярно обновляйте антивирусное ПО на своих устройствах.

***Важно! Расскажите о данных правилах своим близким и пожилым родственникам, чтобы защитить их от интернет-мошенников!***



Соблюдайте эти простые правила, регулярно отслеживайте свою кредитную историю и повышайте свою финансовую грамотность.

# ФОРМА ОБРАТНОЙ СВЯЗИ

**Ф.И.О** _____

_____

Форму обратной связи можно заполнить в электронном формате, пройдя по QR коду*

*Для считывания QR кода с телефона на платформе Android необходимо скачать мобильное приложение по сканированию QR кодов.

**Если Вам не удалось оставить обратную связь по QR коду, Вы можете заполнить анкету ниже:**

Насколько полезны для Вас советы и рекомендации по финансовой и цифровой безопасности?

☐ Полезны на 100% ☐ Полезны на 50% ☐ Бесполезны

Сталкивались ли Вы когда-нибудь с ситуациями, описанными в брошюре?

☐ Да ☐ Нет

Какая тема оказалась наиболее полезной и актуальной?

_____

Какие еще темы были бы Вам интересны?

_____

_____

**Благодарим за предоставление обратной связи!**



**С ЭЛЕКТРОННОЙ ВЕРСИЕЙ БРОШЮРЫ МОЖНО ОЗНАКОМИТЬСЯ ЗДЕСЬ**



Тираж: 300 экз.

Алматы, 2023 г.