Чтобы сохранить свои сбережения и не стать жертвой мошенников, внимательно прочитайте несколько простых правил:

1. Безопасность использования банковских карт (счетов)

•Сотрудники учреждений кредитно-финансовой сферы и платежных систем НИКОГДА не присылают писем и не звонят гражданам с просьбами предоставления данных банковских карт.

•Сотрудник банка НИКОГДА не просит сообщить ему реквизиты банковской карты и совершить какие-либо операции с денежными средствами на банковской карте/счете (например: перевести денежные средства на безопасную ячейку).

•При поступлении телефонного звонка из «банка» и попытках получения сведений о банковской карте, необходимо немедленно прекратить разговор и самостоятельно перезвонить на горячую линию банка, номер которого находится на оборотной стороне Вашей банковской карты, либо обратиться в ближайшее отделение банка.

•Внимательно читайте смс-сообщения, которые поступают Вам на телефон с официального номера банка.

•При поступлении смс-сообщений с неизвестных номеров с текстом «Ваша карта заблокирована», «Заблокирована оплата» и т.п., ни в коем случае не перезванивайте и не переходите по указанным в сообщении ссылкам.

•Если Вам сообщили, что Ваша карта заблокирована, обращайтесь в отделение банка к оператору, кроме того не обналичивайте кредит, который Вы не оформляли, не выполняйте указания человека представившегося оператором.

•Если Вам поступил звонок от «сотрудников банка» о том, что в Вашем личном кабинете оформлена заявка на кредит и денежные средства пытаются похитить мошенники и для сохранности Ваших денежных средств, необходимо перевести денежные средства на «безопасную ячейку» и т.д., НЕМЕДЛЕННО прекратите разговор и обратитесь на горячую линию банка, номер которого находится на оборотной стороне Вашей банковской карты, либо обратиться в ближайшее отделение банка.

2. Продажа/покупка товаров, услуг на сайтах «Авито», «Юла», «BlaBla car»:

•Если Вам пришло смс-сообщение (например об обмене, продаже или покупке товара, выставленного на одном из сайтов) со ссылкой, будьте бдительны и не переходите по данным ссылкам. Если же Вы уже перешли по указанной ссылке и вредоносное приложение установилось на Ваш телефон, немедленно, не запуская его удалите и воспользуйтесь антивирусом, для того, чтоб очистить систему.

•НЕ ВВОДИТЕ реквизиты своей банковской карты на сомнительных сайтах (например: **наложка.рф**)

•НИКОГДА не сообщайте покупателю/продавцу данные своей банковской карты и коды из смс-сообщений.

•При продаже/покупке товаров/услуг на сайтах «Авито», «Юла», «BlaBla car» и др.: ни под каким предлогом НЕ ВВОДИТЕ данные своих банковских карт.

•Не игнорируйте предупреждения о возможных мошеннических действиях на сайтах «Авито», «Юла».

•Самый безопасный способ оплаты товара – после его получения.

3. Использование личного кабинета в онлайн-банке.

•При посещении сайта онлайн-банка обращайте внимание на адресную строку.

•Обращайте внимание на содержание смс-сообщений с кодом-подтверждения операций, вид и сумму платежа. Не вводите код, если есть расхождения в месте проведения платежа.

•Настоятельно рекомендуется использовать на ПК, смартфоне или планшете антивирусное программное обеспечение.

4. Мошенничество через социальные сети «ВКонтакте», «Одноклассники», «Инстаграм».

•Во избежание взлома Вашей страницы в социальных сетях, чаще меняйте пароль и подключите в настройках «двухстороннюю аутентификацию.

•Не переходите по ссылкам, которые скидывают Вам друзья или родственники, а особенно незнакомые люди. Возможно их аккаунты взломали злоумышленники и используют в противоправных целях. Если есть возможность, свяжитесь с другом/родственником напрямую.

•Если Ваш друг пишет с просьбой «одолжить денег» или о том, что какой-либо банк проводить акции и дарит денежные средства, ни в коем случае не предоставляйте данные своей банковской карты и не переводите денежные средства. Если есть возможность, свяжитесь с этим человеком напрямую.

5. НИКОГДА не переводите свои денежные средства экстрасенсам и целителям. Если возникла потребность в услугах вышеуказанных лиц, обращайтесь к ним за личной встречей.

6. Если Вам позвонили якобы сотрудники банка или других организаций и сообщают о том, что Вам положена компенсация (за ранее приобретенные медикаменты, некачественный товар, оказанные услуги) и для ее получения Вам необходимо оплатить инкассацию, госпошлину и прочее, ни в коем случае не переводите денежные средства и немедленно ПРЕКРАТИТЕ разговор.

7. Если Вам сообщают, что кто-то из близких попал в беду, ему грозит наказание и для «решения вопроса» необходимо перевести денежные средства или передать через кого-либо незнакомого, немедленно ПРЕКРАТИТЕ разговор и по возможности перезвоните человеку, который якобы попал в неприятную ситуацию.

8. НИКОГДА не передавайте данные и код-доступа для входа в Ваш личный кабинет кредитной организации или сотового оператора.

9. Старайтесь не совершать покупки в сети «Интернет», если продавец требует от Вас 100% оплаты товара, добросовестные продавцы предлагают возможность отправки товара наложенным платежом с приложением описи содержимого.

10. При покупке товаров в сети «Интернет», обращайте внимание на отзывы интернет-магазинов.

11. Если Вы находитесь в поисках работы и Вам предлагают открыть инвестиционный счет, вложив денежные средства в торговую площадку, купить криптовалюту по выгодной цене, ВНИМАТЕЛЬНО изучите деятельность брокера, убедитесь в том, что у компании существует лицензия на ведение брокерской деятельности (сделать это можно на официальном сайте «Центробанка»), прочтите отзывы о данном брокере. НИКОГДА не переходите по ссылкам и НЕ ВВОДИТЕ реквизиты своих банковских карт.