**Правила банковской безопасности**

**Чтобы сохранить ваши банковские карты и счета в безопасности, помните:**

1. Настоящие сотрудники банков и платежных систем НИКОГДА:

- не присылают писем и не звонят гражданам с просьбами предоставления данных банковских карт;

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

Поэтому если Вам позвонили из «банка» и пытаются получить сведения о Вашей банковской карте:

* немедленно прекратите разговор;
* самостоятельно перезвоните на горячую линию банка, номер которого находится на оборотной стороне Вашей банковской карты, либо обратитесь в ближайшее отделение банка.

2. Если Вам поступило смс-сообщение 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.

3. Если Вам поступило сообщение с официального номера банка с текстом «Ваша карта заблокирована», «Заблокирована оплата» и т.п. немедленно перезвоните на горячую линию банка, номер которого находится на оборотной стороне Вашей банковской карты, либо обратитесь в ближайшее отделение банка.

4. Настоящие сотрудники банка НИКОГДА не дают рекомендаций по переводу Ваших средств на другой счет, никогда не информируют по телефону о совершенных Вами или от Вашего имени операциях.

Поэтому, 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;
* Никогда не обналичивайте кредит, который Вы не оформляли, не выполняйте указания человека представившегося оператором.

5. Настоящие сотрудники правоохранительных органов НИКОГДА не занимаются оперативной работой по телефону дежурной службы территориального правоохранительного органа. Поэтому если Вам позвонил человек, представившийся сотрудником полиции, и попросил провести операции с Вашими средствами на счете, НИКОГДА не выполняйте его телефонные указания. Прекратите разговор и сообщите о случившемся по «телефону доверия» или непосредственно в дежурную часть.

6. Настоящие сотрудники Центробанка России НИКОГДА не занимаются финансовыми операциями со средствами физических лиц, то есть, с Вашими. Это не входит в компетенцию Центробанка. Поэтому любой звонок от имени Центробанка – мошеннический.

7. 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.

**Чтобы не быть обманутым при Интернет-покупке, помните :**

* 1. Самый безопасный способ оплаты товара — после его получения.
	2. 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;
	3. НЕ ВВОДИТЕ реквизиты своей банковской карты на сомнительных сайтах (например: наложка.рф);
	4. НИКОГДА не сообщайте покупателю/продавцуданные своей банковской карты и коды из смс-сообщений;
	5. При продаже/покупке товаров/услуг на сайтах «Авито», «Юла», «BlaBla саг» и др.: ни под каким предлогом НЕ ВВОДИТЕ данные своих банковских карт;
	6. Не игнорируйте предупреждения о возможных мошеннических действиях на салах «Авито», «Юла»;
	7. 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.
	8. При покупке товаров в сети «Интернет», обращайте внимание на отзывы интернет-магазинов.

**Знайте , как избежать мошенничества через социальные сети «ВКонтакте», «Одноклассники», «Инстаграм».**

1. Во избежание взлома Вашей страницы в социальных сетях, чаще меняйте пароль и подключите в настройках «двухстороннюю аутентификацию.
2. 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.
3. 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.
4. НИКОГДА не переводите свои денежные средства экстрасенсам и целителям. Если возникла потребность в их услугах -обращайтесь к ним за личной встречей.
5. 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.

**И ещё несколько простых правил**

1. 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.
2. 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.
3. НИКОГДА не передавайте данные и код доступа для входа в Ваш личный кабинет банка кредитной организации или сотовому оператору.