ПАМЯТКА ПО ФИНАНСОВОЙ ГИГИЕНЕ

«Как не попасть «в руки» мошенников»

Дочитайте эту памятку до конца, даже если уверены, что никогда не станете жертвой мошенников.

ЧАСТЬ I. ЧЕГО НЕЛЬЗЯ ДЕЛАТЬ

1. Не поднимайте звонки с незнакомых иностранных номеров *(Эстония, Латвия, Польша и т.д.)*, если у вас нет там контактов, которые могли бы связаться с вами именно в этот момент.

2. Не доверяйте звонкам и сообщениям, поступающим якобы от имени банков, правоохранительных органов, иных государственных структур, без самостоятельной проверки информации.

3. Не разговаривайте с незнакомыми людьми по телефону, с помощью мессенджеров *(Viber, Telegram и др.)* более 10-15 секунд, если речь идёт о ваших финансах, персональных данных или срочных требованиях совершить какие-либо действия.

4. Никому ни под каким предлогом не сообщайте:

- *личный номер паспорта;*
- *реквизиты банковской карты;*
- *CVV/CVC-код;*
- *ПИН-код;*
- *коды из SMS;*
- *логины и пароли от интернет-банкинга;*
- *коды подтверждения из мессенджеров.*

5. Не принимайте самостоятельных решений под давлением, угрозами, срочностью или эмоциональным воздействием *(например, когда утверждают, что вы стали дропом, финансируете террористов или вам грозят тюрьмой, а вашим близким – опасностью).* Обязательно советуйтесь с теми, кому доверяете, и с профессионалами в соответствующей сфере *(найдите быстрый способ позвонить, написать, дать им о себе знать и получить обратную связь)*.

6. Не верьте документам, присланным в Viber, Telegram или других мессенджерах, даже если они якобы подписаны Национальным банком, правоохранительными органами *(ДФР, КГБ, ДФМ, КГК, МВД)* и другими официальными структурами.

7. Не доверяйте фото и видео людей в форме, которые обращаются к вам через Viber, Telegram или другие мессенджеры *(их легко подделать)*.

8. Не доверяйте голосам и видеоизображениям (дипфейкам) родственников, друзей, коллег, полученным по телефону или через мессенджеры, тем более если они ведут себя странно, напуганы или требуют финансовой помощи *(их голос и изображение можно подделать)*. Сбросьте звонок и перезвоните им сами по известному номеру.

9. Не принимайте участие в так называемых «специальных операциях» по «спасению» себя, близких или других людей, о которых вас просят незнакомые лица по телефону или через Интернет.

10. Не производите «обыски» или проверки квартиры по указанию звонящих, не декларируйте никому свои сбережения и ценности.

11. Никогда не передавайте наличные, валюту или драгоценности третьим лицам, включая курьеров, по чьим-либо указаниям – независимо от того, насколько это кажется логичным или «конспиративным».

12. Не участвуйте лично в перевозке или перемещении наличных, иностранной валюты или драгоценностей по городу, внутри страны или за её пределы – даже если предлагают «заработок» или пугают последствиями за отказ от сотрудничества.

13. Никогда не оформляйте кредиты по указанию третьих лиц. Если же кредит уже оформлен, не переводите полученные средства на счета посторонних лиц *(по указанию ваших «доброжелателей»)*.

14. Не переводите ваши денежные средства (сбережения, депозиты) на «безопасные», «резервные», «специальные» или иные счета, указанные незнакомыми лицами.

15. Не возвращайте самостоятельно денежные средства, якобы ошибочно поступившие на вашу карту или номер телефона от незнакомцев. Обратитесь в банк или к мобильному оператору за консультациями и помощью.

16. Не передавайте свои банковские карты, счета и доступ к ним другим лицам, в том числе за денежное вознаграждение.

17. Не соглашайтесь получать денежные средства на свой счет с последующим их переводом третьим лицам.

18. Не регистрируйте ИП или юридические лица, не открывайте банковские счета по просьбе малознакомых либо посторонних лиц.

19. Не устанавливайте по указанию неизвестных лиц программы удаленного доступа или иные приложения по направленным ссылкам.

20. Не реагируйте на предложения «легкого заработка», связанные с переводом, обналичиванием или транзитом денежных средств.

21. Не оформляйте доверенности на незнакомых лиц или по просьбе малознакомых людей на открытие от вашего имени банковских счетов, совершение финансовых операций или предоставление доступа к вашим счетам, не выезжайте для этого за пределы страны.

22. Не вносите предоплату за товары или услуги, особенно недорогие, предлагаемые через социальные сети *(Instagram, Telegram и другие)*. Это частый способ мошенничества.

23. Не участвуйте в розыгрышах, лотереях и акциях, информация о которых поступила вам по электронной почте, СМС или в мессенджерах от незнакомых отправителей, особенно если для получения «приза» требуется вести банковские реквизиты или данные паспорта.

24. Не откликайтесь на предложения удаленной работы в Интернете, если для трудоустройства вас просят авторизироваться через неизвестные сайты, ввести банковские данные, внести взнос.

ЧАСТЬ II. ЧТО НУЖНО ДЕЛАТЬ

1. Всегда проверяйте информацию, относитесь к ней критически. Если звонят из банка, милиции, следственного комитета, других структур – резко завершите разговор, перезвоните в 102 или самостоятельно по официальному номеру организации, которые легко найти в Интернете на официально сайте. Запомните: сотрудники милиции, КГК и других госорганов никогда не звонят в мессенджерах с требованиями назвать коды, перевести деньги или «помочь в специальной операции».

2. Критически относитесь к любым предложениям «легкого заработка». Предложения получить деньги на свой счет, обналичить их, перевести третьим лицам почти всегда вовлекают в преступную деятельность.

3. При возникновении подозрений, что в отношении вас совершаются мошеннические действия, незамедлительно принимайте следующие меры:

- *заблокируйте банковскую карту через мобильное приложение или по телефону горячей линии банка, а также свои данные в межбанковской системе идентификации;*
- *смените пароли;*
- *обратитесь в банк с заявлением о несанкционированной операции или попытке ее совершения;*
- *сообщите о подозрительных действиях по телефону 102 или в официальный чат-бот МВД в Telegram «Мы всегда рядом»;*
- *подайте письменное заявление в правоохранительные органы.*

4. Проверяйте ссылки и адреса сайтов перед вводом персональных данных, используйте также официальные мобильные приложения банков. При покупках в Интернете проверяйте подлинность ресурса.

5. Используйте базовые меры защиты при работе с банковскими картами:

- *включайте двухфакторную аутентификацию;*
- *устанавливайте лимиты на переводы и снятие наличных;*
- *подключайте SMS- или push-уведомления обо всех операциях по счетам;*

*6. «*Разделяйте» денежные средства:

- *основные накопления храните на отдельном счете (карте);*
- *для текущих расходов используйте другой счет (карту);*
- *для онлайн-платежей применяйте отдельную карту.*

7. Договоритесь с близкими об использовании кодового слова или вопроса, ответ на который известен только членам вашей семьи. При получении подозрительных звонков или сообщений от якобы родственников используйте такие проверочные вопросы.

8. Защищайте свои персональные данные:

- *не публикуйте и не пересылайте фотографии паспорта;*
- *не выкладывайте в социальные сети документы, в которых содержатся персональные данные (ФИО, паспортные данные и т.д.);*
- *ограничивайте доступ к личной информации в соцсетях.*

9. Обучайте близких основам финансовой грамотности. Периодически обсуждайте типичные схемы мошенничества с пожилыми родственниками и подростками.

Особое внимание уделите детям: объясните им, что нельзя общаться с незнакомцами в мессенджерах, устанавливать приложения по их просьбе или передавать деньги курьерам, а также переводить их по предложенной третьими лицами инструкции. Если ребенок столкнулся с подозрительными сообщениями – он должен немедленно рассказать об этом родителям.