**ПАМЯТКА**

**по основным правилам информационной безопасности.**

1. ВСЕГДА проверяйте данные отправителя в мессенджерах, от кого пришло сомнительное сообщение (зайдите в описание аккаунта пользователя и просмотрите полную информацию - убедитесь, что публичное имя пользователя вида «**Имя Фамилия**» и привязанные к нему реальные данные (номер телефона и наименование аккаунта вида **@NameFIO**) соответствуют тем, которые указаны в вашем списке контактов на вашем телефоне.

У поддельных аккаунтов с настоящим совпадает только «**Имя Фамилия**» (номер телефона и наименование аккаунта вида **@NameFIO** будут неизвестные, не из вашего списка контактов, часто - из другого региона РФ или другой страны).

Если аккаунт по всем признакам настоящий, но есть сомнения в полученном запросе (например, начальник или родственник внезапно просит денег или перейти по какой-то странной ссылке с иностранными адресами сайтов) – позвоните отправителю и уточните в личном разговоре.

Очень много случаев взлома аккаунтов и последующих фальшивых рассылок от имени реальных людей.

2. Никаких «кураторов от спецслужб» по бюджетным учреждениям **не существует**.

Любая информация о деятельности вашего учреждения НИКОГДА и НИКОМУ не предоставляется в устном разговоре по телефону или в переписке по мессенджерам/электронной почте – только уполномоченным лицом учреждения после получения официального письменного запроса от официальных госорганов или вышестоящего руководства.

Официальные представители Центробанка, ФСБ, МВД, прокуратуры и других госорганов **НИКОГДА НЕ БУДУТ ЗВОНИТЬ** по официальным служебным вопросам **на личные** сотовые телефоны граждан, не будут ничего присылать вам или запрашивать от вас какую-либо официальную информацию через любые ИНОСТРАННЫЕ сервисы или мессенджеры.

3. **НИКОГДА** не перезванивайте на пропущенные **неизвестные** номера (особенно из других регионов РФ) – это может быть ловушка с переадресацией на платный номер мошенников.

4. НИКОГДА не переходите по ссылкам из полученных с неизвестных номеров СМС вида «**Вам пришло MMS-сообщение. Для получения пройдите по ссылке…**» - это может быть ловушка с внедрением вирусов на ваш телефон.

5. Любые странные сообщения и СМС с неизвестных номеров, особенно с вложенными файлами или ссылками – **ИГНОРИРОВАТЬ**, не открывать вложения и сразу удалять с телефона!

Неизвестного отправителя подобных сообщений – сразу добавлять в «черный список» вашего телефона.

6. **НИКОМУ и НИКОГДА не диктуйте** по телефону **НИКАКИЕ ДАННЫЕ** вашей **БАНКОВСКОЙ КАРТЫ** (особенно 4-значный PIN-код от банковской карты или 3-значный CSV-код с задней стороны карты, которые должны знать и использовать **ТОЛЬКО ВЫ САМИ**) – реальные работники банков НИКОГДА не будут вам звонить на сотовый телефон и что-то запрашивать УСТНО.

7. **НИКОМУ и НИКОГДА не диктуйте** по телефону и не отправляйте через мессенджеры **НИКАКИЕ КОДЫ и ПАРОЛИ** из любых СМС, полученных на ваш телефон – эти данные из СМС нужны только для введения в поля форм сайтов и банковских сервисов.

8. На вашем компьютере **ОБЯЗАТЕЛЬНО** должны быть установлены антивирусные программы с обновляемыми базами.

9. **НИКОГДА** не устанавливайте сомнительные приложения с неизвестных источников. Установка приложений из других источников, в том числе различных ломаных и пиратских версий, может закончиться тем, что вам придется тщательно чистить компьютер или телефон от вирусов. Используйте безопасные источники приложений и официальные сайты компаний, разработавших приложения.

10. **ВСЕГДА** проверяйте безопасность соединений. Всегда обращайте внимание на то, что написано в адресной строке. Если вы видите, что адрес сайта начинается с HTTPS – все в порядке, это безопасное соединение и здесь можно вводить конфиденциальную информацию. В иных случаях - не рекомендуется.

11. Не вводите никакие пароли и не совершайте покупки в Интернете, используя бесплатный Wi-Fi в общественных местах.

12. Проверяйте любые сообщения с просьбами от друзей и знакомых (личными звонками).

13. Закрывайте свои профили и списки друзей в социальных сетях.

14. Используйте только СЛОЖНЫЕ пароли, РАЗНЫЕ ДЛЯ РАЗНЫХ учетных записей и сервисов. Пользователи, которые используют один и тот же пароль для всех сервисов, при компрометации хотя бы одного из сервисов могут потерять доступ ко всем своим учетным записям. Повторное использование старых паролей или одинаковых паролей для разных сервисов - категорически запрещено.

15. По-возможности, во всех доступных сервисах **используйте** двухфакторную аутентификацию («логин и пароль» + «код из СМС или электронной почты» ).

16. **Не публикуйте** служебные электронные адреса на сторонних сервисах и досках объявлений, в конференциях и гостевых книгах.

17. Звонки и сообщения в мессенджерах:

- проверяйте соответствие публичного имени пользователя в мессенджерах «Фамилия Имя» и имени аккаунта «@name» (у поддельных имя аккаунта не будет соответствовать настоящему, которое указано в адресной книге вашего мессенджера);

- не переходите по подозрительным ссылкам, полученным в мессенджерах;

- не вводите логин и пароль от мессенджеров при переходе по ссылкам;

18. Придумайте слово-пароль, которое будут знать только ваши близкие родственники (для проверки мошенников, имитирующих звонки ваших родственников).

**Будьте бдительны!**

**Мошенники постоянно выдумывают все новые и новые схемы обмана.**