Приложение 2

**Меры по обеспечению безопасности информации**

Хотим напомнить вам о правилах кибербезопасности, которые помогут защитить наши данные от угроз. Пожалуйста, будьте бдительны при работе
с электронной почтой. Вот простые рекомендации по предотвращению угроз безопасности информации:

1. Проверяйте адреса электронной почты отправителя, даже если имя совпадает с известным контактом.

2. Не открывайте письма и чаты от неизвестных отправителей.

3. Осторожно относитесь к письмам с призывами к действиям или темами
о финансах и угрозах.

4. Не переходите по ссылкам в письмах, особенно если они короткие или используют сокращатели.

5. Не открывайте вложения с подозрительными расширениями (.zip, .js, .exe
и т. д.) и документами с макросами.

6. Не подключайте неизвестные внешние носители информации к компьютерам.

7. Используйте надежные пароли, создавая их с нестандартными комбинациями символов.

При получении подозрительных писем обратите внимание:

- Знаком ли вам отправитель?

- Присутствуют ли URL-ссылки?

- Есть ли вложение с расширениями .zip, .js, .exe?

- Просит ли файл включить поддержку макросов?

Если есть сомнения и хоть что-то в письме вызывает у вас подозрение,
то велика вероятность, что это фишинг.

С дополнительной информацией по теме личной информационной безопасности, в том числе по эффективному распознаванию фишинговых писем, можно ознакомиться на следующих информационных ресурсах:

Раздел «Кибербезопасность – это просто!» на Едином портале государственных услуг – https://www.gosuslugi.ru/cybersecurity;

Лендинговая страница в сети «Интернет» – https://киберзож.рф/