

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

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/>;

Рекомендации по защите учетных записей

Для того, чтобы защитить свой аккаунт соблюдайте следующие рекомендации:

1 Создавайте сложные пароли длиной не менее 12 символов с комбинацией букв, цифр и специальных символов. Избегайте простых и легко угадываемых паролей.

2 Не используйте один и тот же пароль для разных учетных записей. Создавайте уникальные пароли для каждой важной учетной записи.

3 Регулярно меняйте пароли каждые 3-6 месяцев и обновляйте их при подозрении на утечку.

4 Используйте надежные менеджеры паролей для их хранения и управления.

5 Активируйте двухфакторную аутентификацию (2FA) на всех доступных платформах.

6 Обновляйте пароли при смене сотрудников или их ролей и следите за управлением доступом.

7 При хранении пароля на физическом носителе, убедитесь, что место его хранения абсолютно безопасно.

С дополнительной информацией по теме личной информационной безопасности, в том числе по созданию надежных паролей и эффективному распознаванию фишинга в интернете, 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/>;