**Рекомендации по обеспечению информационной безопасности.**

**1. Как защититься от мошенников: простые правила.**

Распространенный способ действий мошенников: они обманным путем получают данные для доступа к личным кабинетам и приложениям. Используя нейротехнологии, способны подделывать аккаунты и голоса, создавая видеосообщения, сгенерированные искусственным интеллектом, от имени ваших знакомых и руководителей. Зачастую мошенники представляются сотрудниками различных служб или предлагают финансовые выигрыши. Данный подход известен как социальная инженерия.

Вот несколько советов, которые помогут вам защититься от мошенников:

Будьте бдительны: Если разговор кажется подозрительным, завершите его и перезвоните в организацию по официальным номерам.

* Проверяйте способ связи: мошенники часто используют мессенджеры, тогда как настоящие представители не звонят через WhatsApp или Telegram.
* Не сообщайте логины и пароли: читайте назначение смс-кодов и не делитесь ответами на контрольные вопросы.
* Следите за актуальностью номера: убедитесь, что номер, к которому привязан аккаунт, актуален.
* Используйте сложные пароли: меняйте их регулярно и подключайте двухфакторную аутентификацию.
* Проверяйте адрес страницы: убедитесь, что сайт - это официальный ресурс (например, gosuslugi.ru).

Госуслуги обеспечивают защиту, но злоумышленник может получить доступ только при передаче вами необходимых данных. Будьте внимательны и защищайте свои данные.

**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 (.ziр, .js, .ехе 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, .ехе?
* 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.

**3. Рекомендации по защите учетных записей**

Для того, чтобы защитить свой аккаунт соблюдайте следующие рекомендации:

* Создавайте сложные пароли длиной не менее 12 символов с комбинацией букв, цифр и специальных символов. Избегайте простых и легко угадываемых паролей.
* Не используйте один и тот же пароль для разных учетных записей.
* Создавайте уникальные пароли для каждой важной учетной записи.
* Регулярно меняйте пароли каждые 3-6 месяцев и обновляйте их при подозрении на утечку.
* Используйте надежные менеджеры паролей для их хранения и управления.
* Активируйте двухфакторную аутентификацию (2ЕА) на всех доступных платформах.
* Обновляйте пароли при смене сотрудников или их ролей и следите за управлением доступом.
* 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 эффективному распознаванию звонков мошенников, 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**](https://www.gosuslugi.ru/cybersecurity)**);**
* **лендинговая страница в сети «Интернет» —** [**киберзож.рф**](https://киберзож.рф/)**.**