**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:

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

2. Проверяйте способ связи: Мошенники часто используют мессенджеры, тогда как настоящие представители не звонят через WhatsApp или Telegram.

3. Не сообщайте логины и пароли: Читайте назначение смс-кодов и не делитесь ответами на контрольные вопросы.

4. Следите за актуальностью номера: Убедитесь, что номер, к которому привязан аккаунт, актуален.

5. Используйте сложные пароли: Меняйте их регулярно и подключайте двухфакторную аутентификацию.

6. 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.

С дополнительной информацией по теме личной информационной безопасности, в том числе по эффективному распознаванию звонков мошенников, 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/.

**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.

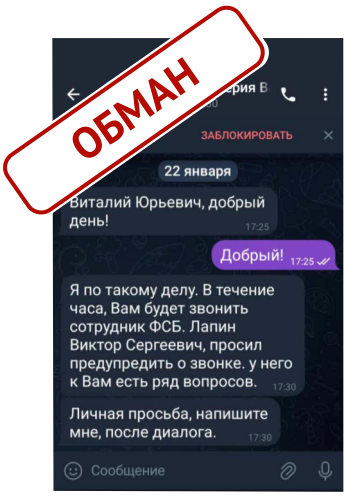
С дополнительной информацией по теме личной информационной безопасности, в том числе по созданию надежных паролей и эффективному распознаванию фишинга в интернете, можно ознакомиться на следующих информационных ресурсах:

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

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

# КАК РАСПОЗНАТЬ ФИШИНГ

## ОТ «РУКОВОДИТЕЛЯ»





**ФИШИНГ** – одна из тактик интернет-мошенников, целью которой является попытка получения конфиденциальных данных, обманом заставлять Вас передать личные и рабочие учетные данные (логины, пароли, пин-коды), нажать на вредоносную ссылку, открыть зараженное вложение или вредоносное приложение.

Фишинговые письма, как правило, имеют характер срочности, сообщая Вам, например, о прекращении доступа к используемому сервису или риске финансовых потерь, а также о необходимости сделать что-то (отправить пароль или данные, перейти по ссылке) как можно быстрее, заставляя мнимой срочностью совершать необдуманные действия.

## УЛОВКИ МОШЕННИКОВ

- подмен номера телефона на официальный
- использование фициальной символики органов государственной власти
- генерация недостоверных голосовых сообщений от лица руководителя
- предоставление фото якобы своего служебного удостоверения
- предоставление фото якобы официального обращения, заверенное подписью и печатью руководителя

## ЧТО ДЕЛАТЬ?

1. СТОП — прекратите какое-либо общение с мошенником
2. не открывать прикрепленные файлы и ссылки из письма (с подозрением на фишинг)
3. сообщите своему непосредственному руководителю о факте обращения от лица руководителя организации
4. дождитесь подтверждения руководителя о достоверности обращения.
5. в случае, если вы подверглись манипуляции и совершили какие-либо действия со своим банковским счетом, немедленно обратитесь в банк для блокирования переводов и в правоохранительные органы – с заявлением о мошенничестве.

## ОБРАЩАЕМ ВАШЕ ВНИМАНИЕ!

ФСТЭК России осуществляет взаимодействие посредством

МЭДО системы МЭДО

почтовой связи

fstec.ru электронной почты (домен @fstec.ru)*

* – при получении электронного письма от имени ФСТЭК России с другого домена, необходимо связаться с ответственным исполнителем по ранее направленным ФСТЭК России письмам, перезвонив по телефону.