Письмо Минцифры России
от 17.09.2024 N П25-305029
<О рекомендациях для государственных служащих, направленных на обеспечение информационной безопасности сотрудников на рабочих местах, личной информационной безопасности>
(вместе с "Как защититься от мошенников: простыми правилами", "Мерами по обеспечению безопасности информации", "Рекомендациями по защите учетных записей")

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО
от 17 сентября 2024 г. N П25-305029

В условиях стремительного развития технологий и увеличения объемов, обрабатываемых данных, защитить личную и служебную информацию становится важной задачей для государственных служащих. Неправильное обращение с информацией может привести к серьезным последствиям, как для отдельных работников, так и для всей государственной службы.

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (далее - Министерство) в рамках федерального проекта "Информационная безопасность" национальной программы "Цифровая экономика Российской Федерации" в период с 2022 по 2024 гг. осуществляет реализацию программы кибергигиены и повышения грамотности граждан Российской Федерации по вопросам информационной безопасности (далее - программа кибергигиены).

Программа кибергигиены реализуется в том числе посредством проведения информационной кампании, включающей в себя мероприятия различного формата, направленные на повышение общего уровня грамотности населения по вопросам информационной безопасности граждан Российской Федерации.

В 2024 году Министерство в рамках реализации Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации, утвержденной распоряжением Правительства Российской Федерации от 22.12.2022 N 4088-р, полагает целесообразным продвижение обучающих материалов по теме информационной безопасности, а также материалов, направленных на непосредственное привлечение внимания к указанной теме.

В связи с этим Министерство подготовило ряд рекомендаций для государственных служащих, направленных на обеспечение информационной безопасности сотрудников на рабочих местах, а также по теме личной информационной безопасности.

На основании вышеизложенного, в целях более широкого информирования сотрудников государственных органов Российской Федерации о значимости соблюдения правил информационной безопасности, просим обеспечить распространение данных рекомендаций среди сотрудников государственных структур.

Врио директора Департамента
обеспечения кибербезопасности
Е.В.ХАСИН

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.

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/.