Приложение

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).

Меры по обеспечению безопасности информации

Напоминаем вам о правилах кибербезопасности, которые помогут защитить ваши данные от угроз. 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.

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.

Рекомендации Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации по эффективному распознаванию фишинговых писем

Фишинг (англ. phishing) — вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей (логин, пароль, номер кредитной карты и другой конфиденциальной информации), а также запуск вредоносного программного обеспечения на компьютере пользователя.

Такой вид интернет-мошенничества, как правило, основан на психологической манипуляции и его цель – вывести человека на такие эмоции, как интерес, страх, жадность, злость, желание помочь. Это позволяет ослабить концентрацию человека, усыпить его бдительность.

Так, применение различных психологических приемов делает такой вид интернет-мошенничества чрезвычайно эффективным, в том числе в организациях.

Пример. Для злоумышленника не составляет труда найти в открытых источниках информацию о структуре Вашей организации, определить ключевых должностных лиц и домен корпоративной почты Вашей организации. Это позволяет злоумышленнику сделать фишинговую рассылку примерно следующего содержания: «Уважаемый ….! В период с 1 марта по 3 апреля Управлением информационных технологий производится ревизия почтовых ящиков сотрудников …. Все неиспользуемые почты будут отключены. Если вы получили данное письмо и планируете использовать данный почтовый ящик в будущем, просьба оперативно войти в личный кабинет по следующей ссылке:……...»

При этом ссылка, конечно же, ведет на поддельную форму авторизации в корпоративную почту. Если тот или иной сотрудник организации вовремя не поймет, что данная рассылка является фишинговой, и перейдет по ссылке, он окажется на странице, которая внешне неотличима от настоящей формы ввода учетных данных. Конечно же, введя логин и пароль, такой сотрудник «добровольно» передаст их злоумышленникам.

Первоначальные действия при получении электронного письма:

Если Вы получили письмо, в котором от Вас требуют какого-либо взаимодействия, в том числе незамедлительного, или же такое письмо вызывает у Вас любопытство, чувство страха или побуждает к действиям, например, «открой», «прочитай», «ознакомься», то задумайтесь и задайте себе следующие вопросы:

ожидаю ли я это письмо?

есть ли смысл в том, что от меня требуют?

знаю ли я автора этого письма?

уверен ли я в безопасности полученного электронного письма?

Если ответ хотя бы на один из озвученных выше вопросов «нет» - внимательно проанализируйте содержимое письма и, при необходимости, свяжитесь для консультации с представителем технической поддержки Вашей организации.

Имейте в виду, что особого внимания требуют письма, которые:

содержат ссылку для перехода на сторонний ресурс (возможно, ссылка ведет на фишинговый поддельный ресурс). При этом еще большего внимания заслуживают письма, содержащие «короткие ссылки», так как невозможно определить, куда ведет такая ссылка;

содержат вложение (возможно, файл содержит вредоносный код для заражения вашего компьютера);

составлены на иностранном языке;

имеют большое количество получателей;

содержат орфографические ошибки;

связаны с финансовой, банковской сферой или геополитической обстановкой.

Как анализировать электронные письма?

1. Проверьте адрес отправителя (домен адреса электронной почты, с которой пришло письмо, должен совпадать с доменом, указанным на официальном сайте организации, от имени которой якобы направлено письмо, а логин такой почты, в свою очередь, должен совпадать с принятой логикой их построения в той или иной организации). Проверяйте адрес отправителя, даже в случае совпадения имени с уже известным контактом;

2. Проверьте полное имя отправителя (для проверки полного имени отправителя, наведите курсор мышки на указанное в письме имя отправителя) и затем проанализируйте высветившийся адрес электронной почты в соответствии с информацией из официальных источников (см. пункт выше);

3. Проверьте, при наличии, ссылки, даже если письмо получено от другого пользователя Вашей информационной системы, и помните о том, что сам факт направления Вам по электронной почте ссылок, ведущих на сторонний ресурс, является подозрительным:

- обратите внимание на название сайта, на который Вам предлагают перейти. В нем может быть изменен порядок букв или, например, некоторые буквы могут быть заменены на цифры (например, www.s0branie.ru). Кроме того, для введения в заблуждение злоумышленником могут быть использованы специализированные сервисы сокращения ссылок (например, bit.ly, tinyurl.com);

- наведите курсор мышки на ссылку (**не нажимая на нее, ссылка появится или рядом с курсором или в левой нижней части окна**) и проверьте, чтобы URL, указанный в электронном сообщении, и URL, отображаемый при наведении курсора на ссылку, совпадали;

- также Вы можете вручную (не копируя ее) вбить полученную ссылку в строке поисковой системы (Яндекс, mail.ru и др.). Такой метод позволит Вам заметить возможные «ошибки» в полученной ссылке;

4. Проверьте наличие вложений. Если отправитель, электронное письмо и причина, по которой Вас просят открыть вложение, вызывает даже самое незначительное подозрение – ни при каких обстоятельствах не открывайте его.

5. Обращайте внимание на возможные опечатки, орфографические ошибки, большое количество прописных букв, совпадение названий организации, имени отправителя и содержимого в тексте электронного письма;

6. Если полученное письмо вызывает сомнения, по возможности, свяжитесь с отправителем или со справочной организации, от которой пришло такое электронное письмо, по другому каналу связи. При этом контактные данные нужно брать из авторитетных источников, например, на официальном сайте организации, а не из направленного Вам письма.

Что делать, если Вы обнаружили фишинговое письмо?

1. Не переходите по ссылке, особенно, если они длинные или, наоборот, созданы при помощи сервисов сокращения ссылок;

2. Не нажимайте на ссылки, если они заменены на слова;

3. Не копируйте адрес ссылки;

4. Не открывайте и не скачивайте вложения, особенно, если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;

5. Не подгружайте картинки от незнакомых людей;

6. Не запускайте макросы в офисных приложениях (макрос – это набор команд и инструкций, группируемых вместе в виде единой команды для автоматического выполнения задачи.);

7. Не пересылайте письма коллегам;

8. Проинформируйте службу технической поддержки своей организации/администратора информационной системы, направив ему полученное письмо **как вложение;**

9. Удалите фишинговое письмо.