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.

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:

проверяйте адреса электронной почты отправителя, даже если имя совпадает с известным контактом;

не открывайте письма и чаты от неизвестных отправителей;

осторожно относитесь к письмам с призывами к действиям или темами о финансах и угрозах;

не переходите по ссылкам в письмах, особенно если они короткие или используют сокращатели;

не открывайте вложения с подозрительными расширениями (.zip, .js, .exe и т. д.) и документами с макросами;

не подключайте неизвестные внешние носители информации к компьютерам;

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:

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;

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 (2FA) 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 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.