ния, максимально приближенные к реальному стилю общения официальных служб поддержки. Такие сообщения могут включать:

- официальный тон, характерный для крупных компаний;

- использование типичных для компании фраз, логотипов, ссылок и даже ссылок на фальшивые, но похожие на официальные веб-сайты;

- персонализированные обращения, где ИИ подстраивается под конкретного пользователя, делая переписку ещё более убедительной.

Сценарии мошеннических действий

В переписке мошенники могут:

уведомлять пользователя о якобы возникшей проблеме с аккаунтом, безопасности или транзакцией;

просить срочно подтвердить личные данные, реквизиты банковских карт или пароли;

предлагать «эксклюзивные» услуги или бонусы, требующие перехода по предоставленным ссылкам;

информировать о необходимости установки обновлений или специальных программ, которые на самом деле содержат вредоносное ПО.

Психологическое воздействие

Использование ИИ позволяет создавать сообщения, которые вызывают у пользователя чувство срочности или тревоги. Например, в сообщениях могут содержаться угрозы блокировки аккаунта или потери доступа к сервису, если не будут выполнены указанные инструкции. Это заставляет человека действовать быстро, не успевая тщательно проверить подлинность сообщения.

Способы защиты

Чтобы минимизировать риск стать жертвой такого обмана, рекомендуется:

проверять источник сообщения: при получении подозрительных сообщений всегда сверяйте информацию через официальный сайт компании или по телефону официальной поддержки;

не переходить по подозрительным ссылкам, если в сообщении присутствуют ссылки, лучше набрать адрес сайта вручную, убедившись в его подлинности;

не передавать личные данные: никогда не отправляйте конфиденциальную информацию (пароли, реквизиты карт, идентификационные номера) через мессенджеры;

использовать двухфакторную аутентификацию – это поможет защитить аккаунты даже в случае взлома пароля;

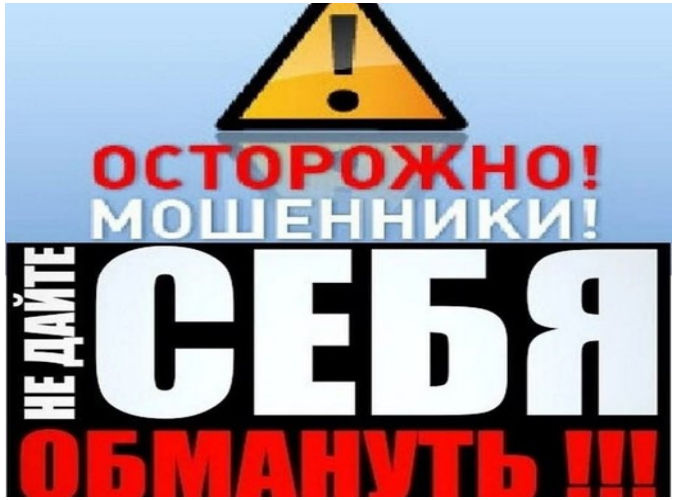
обращать внимание на ошибки: несмотря на высокое качество ИИ, иногда в сообщениях можно заметить несоответствия или ошибки, которые могут указывать на мошенничество.

УМВД России по Тюменской области
625000, г. Тюмень, ул. Водопроводная, 38,
тел. 8 (3452) 793-023 или 102,
тел. 8 (3452) 793-023 или 102
(для абонентов мобильной связи).

Совет при Тюменской областной Думе по повышению правовой культуры и юридической грамотности населения Тюменской области

Управление МВД России по Тюменской области

ПАМЯТКА



ПО ПРОТИВОДЕЙСТВИЮ МОШЕННИЧЕСТВУ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

г. Тюмень, 2025

Используются следующие способы и схемы мошенничества с применением информационно-телекоммуникационных технологий

Подделка квитанций ЖКХ

Злоумышленники рассылают поддельные документы, выглядящие как официальные счета на оплату жилищно-коммунальных услуг. Их цель – заставить получателя перевести деньги на «неправильный» счёт или раскрыть личные и банковские данные.

Как работает мошенничество с поддельной квитанцией?

Подделка оформления. Мошенники тщательно копируют дизайн и элементы настоящих квитанций.

Рассылка через электронную почту или мессенджеры. Поддельные квитанции могут приходить в виде вложений к письмам или сообщений через популярные мессенджеры. Иногда мошенники рассылают SMS с уведомлением об оплате, где содержится ссылка на сайт, внешне напоминающий официальный портал ЖКХ.

Призыв к срочной оплате. В квитанциях часто указывают короткие сроки для внесения платежа, что давит на получателя и заставляет его не вдумываться, а сразу переводить деньги. Иногда дополнительно угрожают отключением услуг или начислением штрафов за просрочку.

Измененные реквизиты для оплаты. Вместо привычных банковских счетов или способов оплаты мошенники указывают реквизиты, принадлежащие им, чтобы переведенные средства оказались у злоумышленников. Также могут использоваться электронные кошельки, перевод на карту или иные методы, усложняющие возврат денег.

Ссылки на поддельные сайты. Вместо настоящих порталов для оплаты квитанций мошенники могут присылать ссылки на поддельные сайты, где просят ввести личные данные или реквизиты банковской карты. Такие сайты часто имеют похожий дизайн, но их цель – сбор информации для дальнейших махинаций.

КАК НЕ СТАТЬ ЖЕРТВОЙ МОШЕННИКОВ?

Проверяйте источник получения квитанций. Если вы получаете квитанцию по электронной почте, убедитесь, что письмо пришло с официального домена вашей управляющей компании или ЖКХ.

При возникновении сомнений не переходите по ссылкам и не открывайте вложения, если не уверены в их подлинности.

Сверяйте данные с предыдущими квитанциями. Обратите внимание на расхождения в оформлении, номерах счетов, реквизитах и контактной информации. Если что-то выглядит иначе, чем обычно, свяжитесь с представителями вашей управляющей компании через официальные каналы (телефон, сайт, личный кабинет).

Осуществляйте оплату через проверенные каналы. Пользуйтесь только официальными сайтами или личными кабинетами для оплаты счетов. Если требуется перевод по реквизитам, убедитесь, что они совпадают с ранее полученными официальными документами.

Не поддавайтесь давлению и требованию моментальной оплаты. Мошенники часто создают искусственную срочность, чтобы побудить вас совершить ошибку.

При малейших сомнениях звоните в свою управляющую компанию или ЖКХ по номерам, указанным на официальном сайте или предыдущих квитанциях. Задайте вопросы о получении квитанции и уточните реквизиты для оплаты.

Защищайте свои электронные устройства. Используйте актуальное антивирусное программное обеспечение и регулярно обновляйте операционную систему. Настройте двухфакторную аутентификацию там, где это возможно, чтобы защитить свои аккаунты от несанкционированного доступа.

Обман с помощью искусственного интеллекта

Обман в популярных мессенджерах с использованием искусственного интеллекта (ИИ) для создания поддельных переписок от лица компаний или службы поддержки.

Такой вид мошенничества представляет собой использование ИИ для создания поддельных переписок в популярных мессенджерах, где мошенники выдают себя за представителей известных компаний или служб поддержки.

Особенности этого вида обмана

Мошенники создают аккаунты или используют существующие мессенджеры для имитации официальных представителей компаний. Это может включать подделку аватаров, имен, описаний профиля и даже использование специальных знаков (например, галочек верификации, если их удаётся подделать). Цель – создать иллюзию доверия и достоверности переписки.

Генерация правдоподобного текста с помощью ИИ. С помощью современных моделей ИИ (например, GPT) мошенники генерируют сообще-