Прокуратура информирует

«Мошенничество с использованием информационных технологий»

В эпоху цифровизации мошенничество становится всё более изощрённым и трудно распознаваемым! Преступники используют самые разнообразные методы, чтобы обмануть людей и получить доступ к их личным данным или финансам.

С любыми онлайн-играми надо быть осторожными, важно помнить о кибербезопасности. Игры-боты в Telegram могут стать инструментом в руках мошенников и киберпреступников.

Рассмотрим типичные риски игр в Telegram

1. Утечка персональных данных

Злоумышленники могут использовать игры-боты в Telegram для получения личных данных. Игра может собирать их через фишинговые ссылки и поддельные запросы на авторизацию либо запрашивать избыточный доступ к информации на смартфоне.

2. Кража аккаунта в Telegram

Для запуска игры используется официальный бот в Telegram, что вызывает доверие пользователей. Но злоумышленники могут обмануть игрока: пообещать ему повышение дохода внутриигровой валюты и попросить для этого войти в игру по фишинговой ссылке.

3. Распространение вредоносного ПО

Злоумышленники могут рассылать вредоносное программное обеспечение под видом приложений для быстрого заработка внутриигровой валюты или её перевода с одного аккаунта на другой. Такое ПО может заблокировать устройство, а затем потребовать выкуп.

4. Мошенничество и финансовые потери

Иногда игры-боты обещают финансовые выгоды, которых в реальности невозможно достичь. Пользователи могут не только тратить время, но ещё и вкладывать деньги, а в итоге не получить никакой выгоды.

За новых людей, привлечённых в игру с помощью уникальной реферальной ссылки, игрок получает игровые бонусы. Но если друзья играми не увлекаются, а рефералы нужны, то игрок может начать их искать в интернете. Например, там предлагают купить их за реальные деньги или совершить сомнительные операции. То есть, игроков мотивируют вложиться в надежде на вывод денежных средств в будущем.

Как защититься

- Защитите свой аккаунт в Telegram и других мессенджерах и онлайн-сервисах. Используйте уникальные и сложные пароли. Включайте двухфакторную аутентификацию (эта распространённая функция защиты работает в Telegram и в WhatsApp), которая затруднит злоумышленникам доступ к вашему аккаунту.
- Никогда не переходите по подозрительным ссылкам и не вводите личные данные на непроверенных сайтах.

- Проверяйте подлинность запросов на авторизацию в мессенджерах, никому не сообщайте код из SMS или приложения.
- Будьте внимательны, предоставляя сторонним приложениям и ботам доступ к вашим данным: местоположению, контактам, фотографиям, платёжным реквизитам, криптокошелькам и др.
- Установите на своё устройство надёжное антивирусное программное обеспечение и регулярно обновляйте его.

Важно помнить, чтобы избежать мошеннических сайтов, следует быть внимательными и осторожными при пользовании интернетом!

Материал подготовлен с использованием информации, размещенной на сайте Сбербанка

Кимрский межрайонный прокурор А.В. Воробьев