Россиянам рассказали, запрос каких разрешений при установке приложения должен вызывать недоверие

Мошенники продолжают совершенствовать свои методы, маскируя вредоносные приложения под полезные сервисы. Часто они используют социальную инженерию, чтобы убедить жертв установить приложение, которое может красть конфиденциальные данные. Как рассказал эксперт по кибербезопасности Александр Ильин, такие приложения часто предлагают якобы полезные функции, например, отслеживание здоровья или дневники питания, а также обещают денежные вознаграждения за простые действия. Другой популярной схемой является рассылка файлов с расширением APK через мессенджеры, с текстами вроде «Ты на фото?» или «Привет, это ты на видео?». При установке этих файлов на устройстве появляется троян, который может перехватывать SMS-коды, фотографии и другие данные.

Одной из новейших угроз является использование NFC-технологии, когда мошенники убеждают пользователя установить вредоносное приложение и приложить банковскую карту к смартфону. Затем они просят ввести SMS-код для авторизации, и в результате создаётся виртуальный клон карты. Такой клон можно использовать для снятия денег через банкоматы с бесконтактной технологией. Эксперт отмечает, что вредоносные приложения часто запрашивают разрешения, которые не соответствуют их функционалу, такие как доступ к SMS-сообщениям, контактам или камере. Это должно насторожить пользователя, ведь такие разрешения могут свидетельствовать о скрытых намерениях.

Чтобы защититься от подобных атак, Ильин советует несколько простых правил. Во-первых, приложения нужно устанавливать только из официальных магазинов, таких как Google Play или App Store. Важно также проверять репутацию разработчика и читать отзывы других пользователей. Во-вторых, необходимо регулярно проверять разрешения, которые приложения запрашивают, и отзывать лишние. Ещё один совет — не сканировать случайные QR-коды, которые могут привести на фишинговые сайты или загрузить вредоносное ПО. Эксперт рекомендует включать многофакторную аутентификацию для важных сервисов, а также устанавливать надёжное антивирусное ПО, которое поможет предотвратить заражение.