АНТИТЕРРОР
УРАЛ

ВРЕДОНОСНЫЕ ПРОГРАММЫ

Киберпреступники маскируют вредоносные программы под полезные файлы.

Нередко вирусы скачивают под видом популярных фильмов, книг школьной программы и полезных приложений.

Как это работает? Преступники создают копии сайтов и размещают их в первых поисковых выдачах браузера. После загрузки файла вредоносная программа крадет пароли, банковские данные и получает полный контроль над устройством.

АНТИТЕРРОР
УРАЛ

ОПАСНЫЕ ПРИЛОЖЕНИЯ

В популярных магазинах приложений преступники размещают копии полезных программ и мобильных приложений.

Остерегайтесь:

- копий приложений известных нейросетей
- пиратских игр
- фейковых фото- и видеоредакторов

Вредоносное приложение зачастую визуально похоже на оригинальное. В названии может быть заменена буква или добавлена приписка новой версии или мода.

АНТИТЕРРОР
УРАЛ

ОПАСНЫЕ QR-КОДЫ

Злоумышленники рассылают объявления о создании чатов для жильцов домов. Для вступления предлагают отсканировать QR-код, который ведет на фишинговые сайты или содержит вредоносное ПО.

Злоумышленники наклеивают фальшивые QR-коды поверх оригинальных на самокатах, сдающихся в аренду.
Эти коды ведут на поддельные сайты, максимально похожие на официальные сервисы проката.

АНТИТЕРРОР
УРАЛ

ФИШИНГОВЫЕ САЙТЫ ИГРОВЫХ ПЛАТФОРМ

Как действуют преступники? Кибермошенники используют новую схему для обмана детей и подростков с помощью фишинговых сайтов, которые как две капли воды похожи на официальные страницы игровых платформ.

Попытка авторизации на таком сайте приводит к потере личных данных, краже игровой валюты и персонажей, денег с привязанных карт.

Распространяют ссылки на такие сайты в игровых чатах и форумах, а также запрещенных в России мессенджерах.

АНТИТЕРРОР
УРАЛ

Чтобы обезопасить себя от киберугроз, соблюдайте следующие меры предосторожности:

- внимательно проверяйте адреса посещаемых сайтов и предлагаемые сервисы — даже одна лишняя буква может означать подделку
- не переходите по ссылкам из подозрительных сообщений и соцсетей
- используйте антивирусы, которые вовремя уведомят о вредоносном сайте и не дадут установить вирус на ваше устройство

АНТИТЕРРОР
УРАЛ

БЕЗОПАСНОСТЬ ПАРОЛЕЙ

- Используйте специальные приложения для хранения паролей от проверенных антивирусных программ
- Устанавливайте сложные и длинные пароли
- Ежемесячно меняйте пароли
- Включите двухфакторную аутентификацию
- Не снимайте на камеру свои пароли. Современные вирусы научились распознавать текст и в некоторых случаях подчерк
- Не используйте один пароль для всех приложений и сайтов