

Как мошенники обманывают исполнителей и заказчиков

Предоплата за доступ к работе



Вы встречаете **объявление с привлекательными условиями работы**. Но чтобы получить доступ к проекту, нужно внести предоплату. Как правило, фейковый работодатель говорит, что требуется купить программное обеспечение или дорогие инструменты.

Бесплатные тестовые задания



Вы можете **несколько часов или даже дней выполнять работу**, за которую вам не заплатят. «Заказчик» будет использовать тестовый дизайн или текст, но исполнитель ничего за это не получит.

Фейковые аккаунты и накрутка рейтингов

РФ

Вы можете **найти отличного исполнителя за адекватные деньги**, но все отзывы и рейтинги окажутся накрученными. Заказчик получит некачественную работу или исполнитель вообще исчезнет после получения предоплаты: прекратит переписку и удалит аккаунт.



Поддельные платёжки и квитанции



После того как вы выполните работу, заказчик **пришлёт вам поддельную квитанцию** или платёжный документ и скажет, что перевёл вам деньги. Но вам ничего не придёт.

Атаки на аккаунты



Мошенники **взламывают аккаунты** проверенных исполнителей или заказчиков, а затем используют их репутацию, чтобы привлекать клиентов, требовать предоплату или получать платежи за фальшивые заказы.

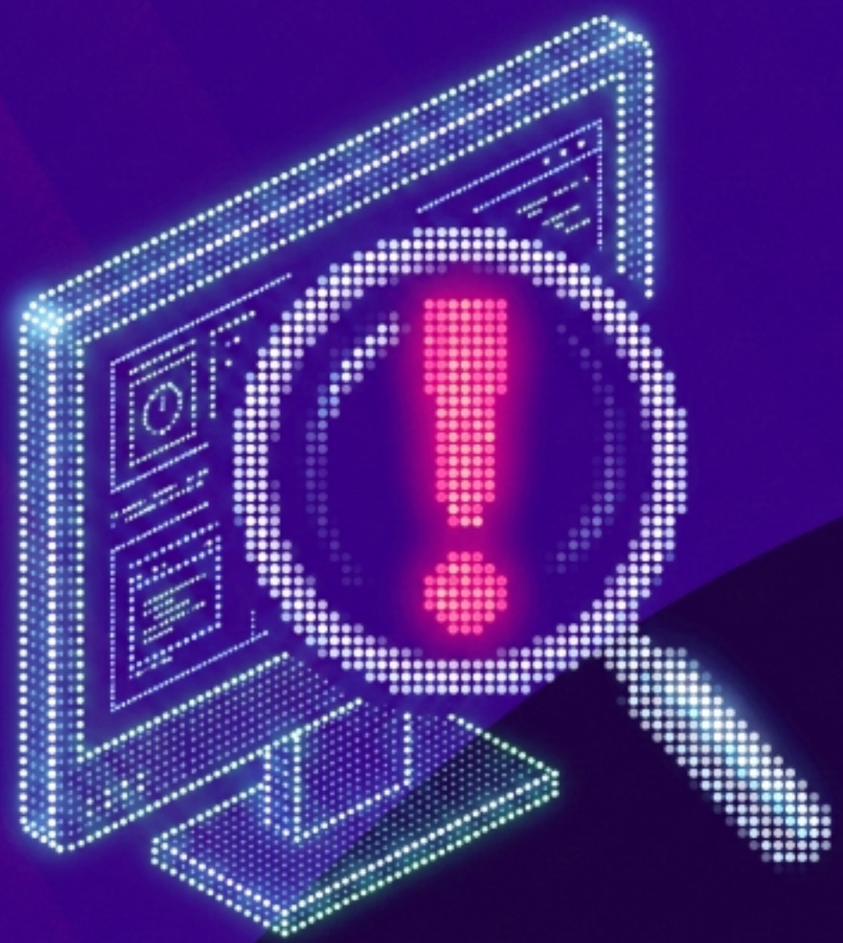
Фишинговые ссылки и вредоносное ПО

РФ



Преступники могут **отправлять фишинговые ссылки**, маскируя их под важные файлы или проектную документацию. Перейдя по ним, пользователи заразят гаджет вирусами.

Как защитить себя



Изучайте репутацию заказчика или исполнителя: осторожно относитесь к аккаунтам с очень высоким рейтингом или однотипными отзывами.



Работайте через **официальные платформы**, никогда не переходите в сторонние мессенджеры, не принимайте оплату переводом.

Проверяйте все транзакции.