1.Сделать двойную аутефикацию при входе

2.С помощью ввода сложного пароля и подтверждением кода присланного на телефон

3.Для защиты от подобных атак рекомендуется в первую очередь избегать установки приложений из недоверенных источников. С осторожностью необходимо устанавливать также приложения с подозрительными названиями даже из официальных магазинов, поскольку никакие проверки, организованные администрацией этих магазинов, не могут работать идеально. Своевременно обновляйте ОС и приложения, чтобы исключить возможность атак через известные уязвимости.

4.В первую очередь, будьте внимательны и не оставляйте телефон и планшет без присмотра в общественных местах. Обязательно установите пароль для разблокировки устройства или включите биометрическую защиту, если это возможно. Не повышайте привилегии до административных (jailbreak или root), отключите отображение уведомлений на заблокированном экране.

5.Могут представиться сотрудниками и требовать данные которые не имеют права спрашивать у пользователя. В таких случаях можно просто положить телефон (если это звонок)

6.Клиент может говорить что транзакция прошла, но ничего нету. Так же может поделать данные.

7.Усилить подтверждения пользователя и шифрования данных

8.DoS-атака которая может привести к падению серверов и компании