

Установил подозрительную программу



Особенно важно действовать отдельно, если собеседник видел экран или управлял устройством.

СДЕЛАЙТЕ СЕЙЧАС

Остановите удалённый доступ и отключите подозрительное устройство от сети.

1. Не открывайте на нём банк и не вводите новые пароли. Для срочных действий используйте другое безопасное устройство.
2. Если затронуты банковские операции или коды, самостоятельно свяжитесь с банком и сообщите об установленной программе.
3. С безопасного устройства проверьте важные аккаунты: контакты восстановления, неизвестные входы и выданные разрешения. Смените раскрытые пароли.
4. Сохраните название программы и обстоятельства установки. Разберитесь удаление программы и выданных ей прав с доверенным специалистом; одно удаление не доказывает, что все доступы отозваны.

Чего не делать

Не устанавливайте второй «антивирус от поддержки» из той же переписки и не оплачивайте обещание гарантированно очистить устройство.

Официальная справка

- [Microsoft: Защита компьютера от нежелательных программ](#)
- [Microsoft: Защита от вирусов и угроз в Безопасности Windows](#)
- [Т-Банк: Что делать, если перевели деньги мошенникам](#)

Полная инструкция и все источники: learn.ivan-it.net/help/app/

Поддержка сайта: sos@ivan-it.net. Школа не заменяет банк, оператора или полицию. Редакция 30 октября 2026 года.