

# Основные методы интернет-мошенников

1. Угроза безопасности
2. Манипуляция здоровьем близких
3. Создание профилей-двойников
4. Внушение ложной надежды



## Как защититься от мошенников

1. Не ищите легкой наживы
2. Проверяйте любую информацию
3. Не сообщайте посторонним лицам свои персональные данные
4. Не переходите на сайты однодневки (Фишинговые сайты)



### Контактная информация

ЧПОУ Вологодский  
кооперативный колледж  
Студент группы Ю-12  
Поспелов Кирилл

[pospelovkirill41@gmail.com](mailto:pospelovkirill41@gmail.com)

**Кибербезопасность.  
Как не стать  
жертвой  
мошенников в  
интернете?**

## Что такое кибербезопасность?

Понятия «кибербезопасность» и «информационная безопасность» довольно часто используются в качестве синонимов. Однако в действительности эти термины сильно различаются и не являются взаимозаменяемыми.

## Понятие кибербезопасности и информационная безопасность одно и то же?

Понятия «кибербезопасность» и «информационная безопасность» довольно часто используются в качестве синонимов. Однако в действительности эти термины сильно различаются и не являются взаимозаменяемыми.



## Цели кибербезопасности

Основной целью кибербезопасности является предотвращение кражи или компрометации информации. Важную роль в достижении этой цели играет триада безопасной IT-инфраструктуры — конфиденциальность, целостность и доступность.

## Что делать если вы стали жертвой мошенников?

- 1 Собрать доказательную базу: выписка с банковского счета, в идеале — запись телефонного разговора с мошенником.



- 2 Подайте заявление в МВД по месту своего жительства. Предварительно можете позвонить по телефону горячей линии госоргана 8 800 222 74 47.
- 3 Ждите вызова и расследованиям