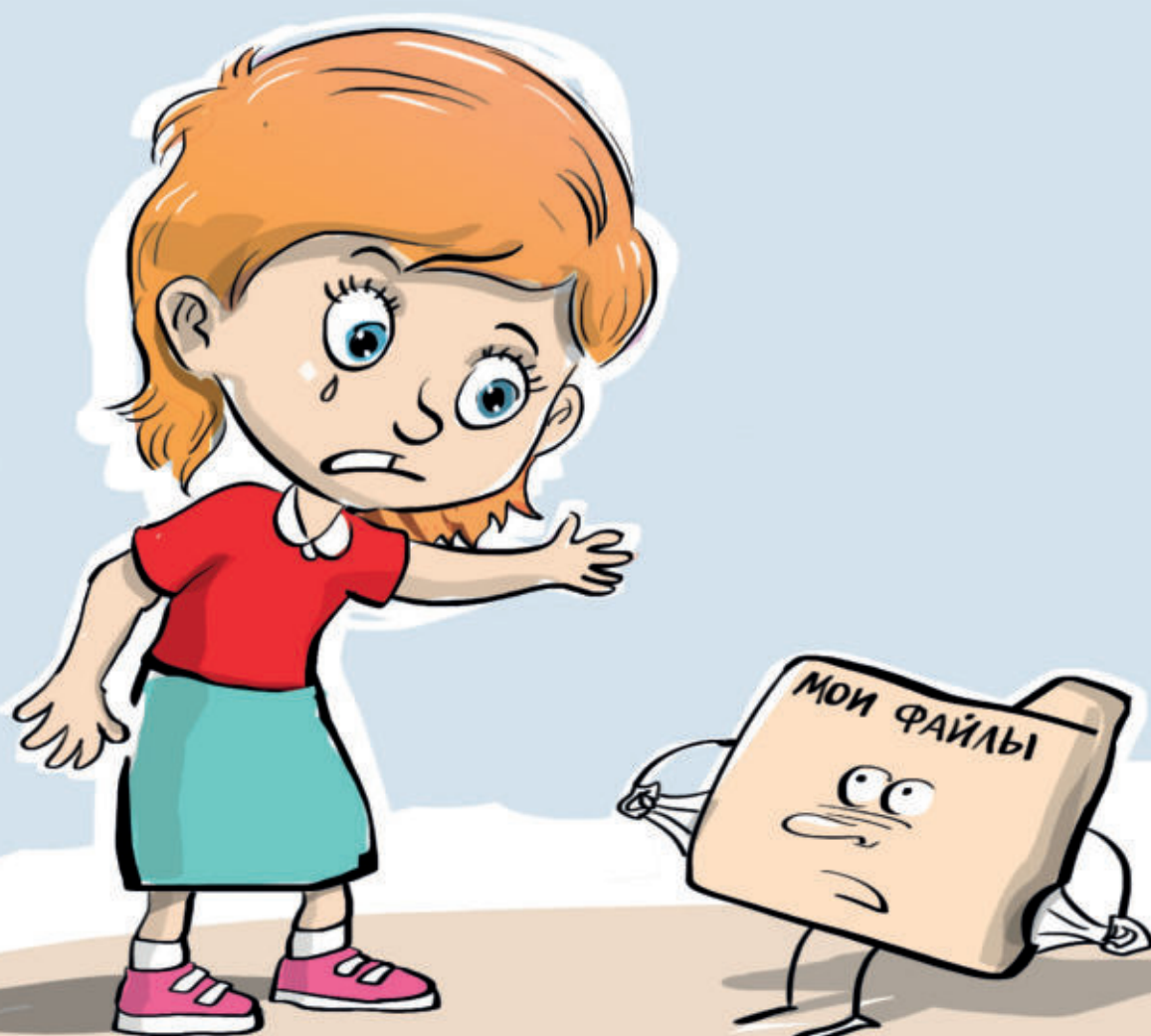


# ЧТО ТАКОЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ



НАЦИОНАЛЬНЫЙ  
ЦЕНТР ПОМОЩИ  
ПРОПАШИМ И ПОСТРАДАВШИМ ДЕТЯМ  
НАЙТИРЕБЕНКА.РФ



лига  
безопасного  
интернета



Сайт  
[ligainternet.ru](http://ligainternet.ru)

**Персональные данные – это все ключевые и важные сведения о человеке. Их следует тщательно беречь и не раскрывать в Интернете без необходимости. Раскрытие персональных данных в Интернете может привести к очень неприятным последствиям: нежелательным звонкам, спаму, краже аккаунтов, мошенническим действиям, вымогательству денег у тебя или твоих близких, угрозах совершения компрометирующих тебя действий, краже денег и документов. В некоторых случаях это даже может привести преступника на порог твоего дома.**

## **Что относится к персональным данным?**

- 1. Фамилия, имя, отчество;**
- 2. Все твои документы** (паспорт, свидетельство о рождении, аттестат и др.);
- 3. Банковские данные** (номер счета, карты, пин-код, CVV-код);
- 4. Твоя контактная информация** (номер телефона, адрес электронной почты, адрес места жительства, работы или учебы);
- 5. Фотографии и видеозаписи с твоим изображением;**
- 6. Данные о твоих родственниках;**
- 7. Твои логины и пароли.**

Чаще всего пользователи сети сами выкладывают информацию о себе в Интернет. Мошенники охотятся за этими данными. Большинство информации о жертвах преступники находят в открытом доступе в соцсетях и в Интернете.

## **Как защитить свои персональные данные?**

- 1. Придумывай и используй разные сложные пароли для почтовых ящиков, соцсетей и других сайтов.** Пароль восстановить проще, чем вернуть украденные деньги.
- 2. Не выкладывай в соцсети и не отправляй друзьям фотографии и номера своих документов, карт и билетов.**
- 3. Не отмечай местоположение** своего дома, работы, учебы, маршрутов прогулок, в том числе, под фотографиями и видеозаписями.
- 4. Не ставь в браузере «разрешить» всплывающим окнам.** Сначала внимательно прочитай короткое сообщение перед тем, как давать доступ и соглашаться на какое-либо действие.
- 5. Проверь, чтобы твои аккаунты не были доступны с чужих устройств.** В настройках безопасности можно посмотреть историю входов. Если ты обнаружил выполненный вход на постороннем устройстве, сразу же удали это устройство из списка.
- 6. Закрой доступ к своим страницам в социальных сетях.** Включи настройки конфиденциальности.

**МОШЕННИКИ ИЗОБРЕТАТЕЛЬНЫ,  
НО ВСЕГДА ПОБЕДИМЫ!**