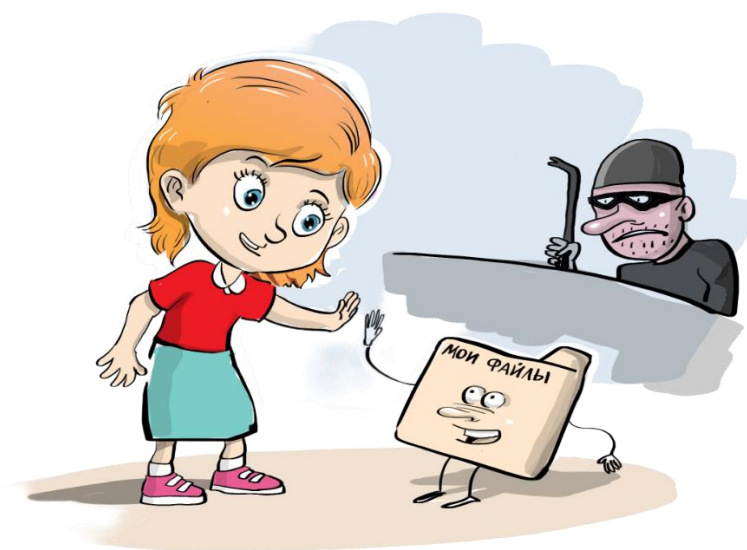




ТОГБУ «Центр поддержки семьи и помощи детям
«Семейный причал»
Служба постинтернатного сопровождения выпускников

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.

Твои персональные данные – что
это и как их защитить?





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?

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

