**Что такое персональные данные и как с ними обращаться?**

Персональные данные – это любая информация, которая относится к тебе: имя, фамилия; дата рождения; номер школы; номер телефона; твой адрес и другая личная информация.

Персональные данные в интернете нужны для того, чтобы зарегистрироваться на сайте или в социальных сетях, для того чтобы делать покупки или играть в игры. Но, есть данные, которыми мы можем делиться случайно!

Задумайся! Это тоже персональные данные, их нужно хранить от незнакомых людей: место нахождения; места учебы; пароли; данные банковских карт родителей; спортивные секции, или другие группы, в которых ты участвуешь.

**Правила безопасности**

Всегда проверяй надежность сайта перед регистрацией. Обрати внимание на тревожные звоночки:

* Ошибки в названии сайта;
* В адресе сайта содержится много цифр и случайных символов;
* На сайте открывается множество дополнительных окон.

**Оберегай свой компьютер**

* Для защиты своего компьютера необходимо регулярное обновление программного обеспечения, использование надежных антивирусных
и антишпионских программ;
* Устанавливай такие программы только с официальных сайтов;
* Постоянно обновляй антивирусные программы;
* Познакомь с этими программами своих родителей, чтобы они помогли защитить твой компьютер.

**Будь внимателен, переходя по ссылкам**

* Критически относись к сообщениям, которые прислали незнакомцы, к яркой рекламе, всплывающей на разных сайтах. Ты никогда не угадаешь, что на самом деле тебя там ждёт (вирусы, вредоносная
и неприятная информация);
* Попадая случайным образом на такие странички следует немедленно их закрыть, ничего не загружать.

**Такие ссылки можно узнать по некоторым признакам**

* Очень яркие баннеры;
* Сложные, непонятные адреса;
* Ошибки в названии;
* Нереалистичные обещания;
* Обещания бесплатной награды за переход по ссылке или скачивание;
* Необходимость отправлять СМС для скачивания.

**Прояви осторожность в подключении к общественным сетям Wi-Fi**

Бесплатные и общественные сети часто бывают незащищенными, в них нет возможности ограничить себя от вредоносных программ и действий злоумышленников. Подключайся к такой сети только в случае крайней необходимости. Контролируй вход и выход из своих аккаунтов. Всегда выходи из системы после завершения работы. Особенно если ты пользовался компьютером вне дома.