

## Интернет-самозащита для обучающегося

Если ты заводишь страничку в социальной сети, то первым делом ты должен решить – у тебя будет публичный аккаунт или приватный. Сегодня есть такая профессия – блогер, и многие хотят ими быть, но нельзя сидеть на двух стульях и рассчитывать на то, что и вас будут лайкать все подряд, и аккаунт будет приватным.

Соответственно, если аккаунт предполагается **публичным**, в нем следует повесить только свою фотографию, назвать имя-фамилию или назваться так, как вы бы хотели, чтобы вас называли, и больше никаких данных не публиковать. В друзья в публичный аккаунт добавляют обычно тех, кто нужен, чтобы его раскручивать, и в целом к ведению этой странички следует относиться как к работе. Публичный аккаунт – это как сцена, на которую ты выходишь, и перед тобой сидит аудитория незнакомых людей. Есть некоторая вероятность, что после этого «выступления» они начнут задавать вопросы, но все это должно происходить не в личных сообщениях, а в публичных комментариях – это же работа, а если общение переходит в личную зону, оно должно продолжаться в тех же рамках, каких оно придерживается в публичном пространстве.

Если ты решаешь, что аккаунт **приватный** и что ты хочешь его использовать для общения со своими одноклассниками, родителями, друзьями и прочими, ты должен сразу пойти в настройки и сделать так, чтобы страничка была доступна только для друзей.

***Относись к интернету как к реальному миру и сравнивай поступки, которые ты совершаешь в интернете, с тем, что ты делаешь в реальной жизни.***

Готов ли ты запускать в свой дом, в свою комнату всех подряд? Так же и в интернете: твой приватный аккаунт – это твой дом, и не следует туда пускать незнакомцев, и вряд ли стоит размещать фото и видео, где ты делаешь что-то или выглядишь так, что, это может скомпрометировать тебя и твою репутацию.

Дружить в приватном аккаунте стоит только с теми, кого ты знаешь в реальном мире или с теми, с кем ты бы мог познакомиться в реальном мире. Например, твоя подруга ходит на курсы французского и решает познакомить тебя со своим другом из группы. Лет 15 назад ей бы пришлось вас обоих звать в кино или в кафе, а сейчас она кинет ему ссылку на твой аккаунт, тебе – на его, и вот вы подружились. Это совершенно нормальная ситуация.

Во всех остальных случаях с незнакомыми людьми в социальных сетях общаться нельзя, потому что у нас там обычно много персональных данных: например, 20% подростков публикуют в аккаунте номер телефона, а 80% указывают номер школы. Кстати, когда ты размещаешь персональную информацию и личные фотографии на своей закрытой страничке и считаешь, что она таким образом защищена, не забывай, что аккаунты сплошь и рядом

взламывают – наверняка ты часто слышишь о таких случаях, и вся информация становится доступна неизвестно кому.

Анонимно можно общаться вне социальных сетей с кем угодно, но если ты это делаешь, ты не делишься персональной информацией, не сообщаем свое имя и фамилию, потому что по именам и фамилиям в соцсетях можно легко найти человека.

*Не общайся в приватном пространстве с незнакомыми людьми и всегда имей в виду, что никогда нельзя быть уверенным в том, что человек – тот, за кого он себя выдает. Мы, конечно, всегда ищем для себя наиболее комфортное объяснение и думаем: да нет, вряд ли это маньяк-педофил, наверное, у него просто нет друзей, или я ему просто понравилась, он где-то нашел мою фотографию, я такая классная, но проблема в том, что мы никогда не получим достоверного ответа на этот вопрос.*

## Интернет-гигиена

Не реагируй ни на какие просьбы срочно переслать деньги или перейти по какой-то ссылке – ни в социальной сети, ни в электронной почте. Ходи по проверенным страницам с включенным антивирусом, потому что вирусы заражают и большие сайты!

*Это миф, что вирусы водятся только на каких-то подозрительных порнографических страницах, и если туда не ходить, то все будет в порядке.*

Антивирусная программа дает 99,999...% гарантии – но всегда есть новые программы, которые еще не успели добавиться в базу.

Чтобы защититься от них, не ходи по баннерным сетям и не кликай на них, не ищи, где скачать бесплатно новые фильмы. Для безопасного скачивания софта следует пользоваться не торрентами, а сайтами разработчиков, для просмотра фильмов – лицензионными видео-сервисами. Это то, что называется базовой интернет-гигиеной. Помни, что в интернете, как и в реальной жизни, есть мошенники. Не бросайся покупать что-то, что тебе обещают в три раза дешевле, отнесись с подозрением к сообщению от друга с просьбой кинуть туда-то 50 рублей или проголосовать за него – не ленись уточнить, например, в WhatsApp, от него ли это сообщение, потому что, как правило, это мошеннические схемы.