Кибербуллинг, или виртуальное издевательство

Кибербуллинг **— преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.**

Основные советы по борьбе с кибербуллингом:

1. **Не бросайся в бой. Успокойся. Если ты начнещь отвечать оскорблениями на оскорбления, только больше разожжешь конфликт.**
2. **Управляй своей киберрепутацией.**
3. **Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.**
4. **Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.**
5. **Веди себя вежливо. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.**
6. **Ограничь доступ агрессору. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.**
7. **Если ты являешься свидетелем кибербуллинга, твои действия следующие: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь.**

Адрес: 630099, г. Новосибирск, ул. Советская, 33, а/я 325.
Тел.: +7(383)349-55-89
E-mail: rsockanc54@rkn.gov.ru

Управление Роскомнадзора по Сибирскому федеральному округу

Как защитить свои персональные данные в Интернете

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ.
2. Постоянно устанавливай обновления, которые автоматически устанавливаются с целью доработки программы, и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика операционной системы. Если существует режим автоматического обновления, включи его.
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере.
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз.
5. Ограничь физический доступ к компьютеру для посторонних лиц.
6. Используй внешние носители информации, такие как флешка, диск или файл из Интернета, только из проверенных источников.
7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислали твои знакомые. Уточни, отправляли ли они данные файлы.

Советы по безопасности работы в общедоступных сетях Wi-fi:

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-либо номера.
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на свое устройство.
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе.
4. Не используй публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту.
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://».
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Основные советы для безопасности мобильного телефона:

1. Будь осторожен, ведь когда предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Обновляй операционную систему смартфона.
4. Используй антивирусные программы для мобильных телефонов.
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.
6. После того как выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
7. Периодически проверяй, какие платные услуги активированы на номере твоего мобильного телефона.
8. Давай свой номер мобильного телефона только людям, которых знаешь и кому доверяешь.
9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.