ПАМЯТКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ СТУДЕНТОВ

Юлия Конанова и
Фунтикова Елена
ФЖ-21-17

Запрещается:

- 1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию, телефон, адрес, название учебного заведения, а также фотографии свои, своей семьи и друзей);
- 2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
- 3. Грубить, придираться, оказывать давление - вести себя невежливо и агрессивно в сети;
- 4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда ставь в известность родителей;
- 5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым человеком, которому доверяешь.

Осторожно:

- 1. Не все пишут правду. Читаешь о себе неправду в Интернете - сообщи об этом своим родителям или опекунам;
- 2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
- 3. Незаконное копирование файлов в Интернете - воровство;
- 4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
- 5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

Можно:

- 1. Уважай других пользователей;
- 2. Пользуешься Интернет-источником - делай ссылку на него;
- 3. Открывай только те ссылки, в которых уверен;
- 4. Обращаться за помощью - родители, опекуны и администрация сайтов всегда помогут;
- 5. Пройди обучение на сайте "Сетевичок" и получи паспорт цифрового гражданина!
- Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином!
- *ИНФОРМАЦИОННАЯ ПАМЯТКА ДЛЯ ОБУЧАЮЩИХСЯ ПО ИСПОЛЬЗОВАНИЮ СОЦИАЛЬНЫХ СЕТЕЙ*Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.
-

Основные советы по безопасности в социальных сетях:

- 1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
- 2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты планируешь провести свободное время;
- 3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
- 4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- 5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- 6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- 7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда, если тебя взлома**ют, то злоумышленники получат доступ только к одному месту, а не во все сразу.**
-

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. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале нужно успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще 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. Соблюдай свою виртуальную честь смолоду;
- 6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
- 7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
- 8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить о факте агрессивного поведения в сети.

Общие правила для родителей :

- Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
- Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
- Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
- Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
- Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Советы по безопасности работе 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-то номера; 2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твое 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.

Авторское право:

- Современные школьники, студенты – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность. Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями. Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете. Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установленный не легальная программа. Не стоит также забывать, что су ществует легальные и бесплатные программы, которые можно найти в сети.