

КАК БЕЗОПАСНО ОБЩАТЬСЯ В СОЦИАЛЬНЫХ СЕТЯХ

Эта памятка поможет тебе безопасно общаться в социальных сетях

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.

Советы по безопасному общению 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 и твои родители планируете провести каникулы.
- 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 информацию: 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 взломают, то злоумышленники получат доступ только к одному месту, а не ко всем сразу.

КАК ЗАЩИТИТЬСЯ ОТ КОМПЬЮТЕРНЫХ ВИРУСОВ

Эта памятка поможет тебе безопасно находиться в сети

Компьютерный вирус – это программа, отличительной особенностью которой является способность к размножению. Вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена зараженная программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ

- 1** Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ.
- 2** Постоянно устанавливай патчи (цифровые заплатки для программ) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. 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 твоём 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 ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРБУЛЛИНГА

Эта памятка поможет тебе защититься от виртуальных издевательств

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

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 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. Соблюдай свою виртуальную честь смолоду.
- 5** Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
- 6** Бань агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.
- 7** Твои действия, если ты свидетель кибербуллинга: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

КАК ЗАЩИТИТЬСЯ ОТ КИБЕРБУЛЛИНГА

Эта памятка поможет тебе защититься от виртуальных издевательств

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

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 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. Соблюдай свою виртуальную честь смолоду.
- 5** Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
- 6** Бань агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.
- 7** Твои действия, если ты свидетель кибербуллинга: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

КАК БЕЗОПАСНО ПОЛЬЗОВАТЬСЯ СМАРТФОНОМ, ПЛАНШЕТОМ

Эта памятка поможет тебе безопасно пользоваться мобильными устройствами

Смартфоны и планшеты содержат в себе взрослый функционал и могут конкурировать со стационарными компьютерами. Однако средств защиты для подобных устройств пока мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Советы по безопасному использованию мобильных устройств

- 1** Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе 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** Необходимо обновлять операционную систему твоего 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 ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
- 7** Периодически проверяй, какие платные услуги активированы на твоём номере.
- 8** Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
- 9** Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

КАК БЕЗОПАСНО ИГРАТЬ ONLINE

Эта памятка поможет тебе безопасно играть в интернете

Online-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Меры защиты твоего игрового аккаунта

- 1** Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.
- 2** Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов.
- 3** Не указывай личную информацию в профайле игры.
- 4** Уважай других участников по игре.
- 5** Не устанавливай неофициальные патчи и моды.
- 6** Используй сложные и разные пароли.
- 7** Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГА

Эта памятка поможет тебе защитить личные данные

Обычной кражей денег и документов никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг (от английского слова **fishing** – рыбная ловля), главная цель которого состоит в получении конфиденциальных данных пользователей – логинов и паролей.

Советы по борьбе с фишингом

- 1** Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
- 2** Используй безопасные веб-сайты, в том числе интернет-магазинов и поисковых систем.
- 3** Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.
- 4** Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзья, о том, что тебя взломали и, возможно, от твоего имени будут рассылаться спам и ссылки на фишинговые сайты.
- 5** Установи надежный пароль (PIN) на мобильный телефон.
- 6** Отключи сохранение пароля в браузере.
- 7** Не открывай файлы и другие вложения в письмах, даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

КАК ОБЕСПЕЧИТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕБЕНКА

Эта памятка поможет обеспечить информационную безопасность вашего ребенка

Общие правила:

- 1** 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.
- 2** Если ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и другие), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
- 3** Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Странички вашего ребенка могут быть безопасными, но могут содержать и ссылки на нежелательные и опасные сайты (например, порносайт или сайт, на котором друг упоминает номер сотового телефона вашего ребенка или ваш домашний адрес).
- 4** Поощряйте вашего ребенка сообщать обо всем странном или отталкивающем и не слишком остро реагируйте, когда он это делает (из-за опасения потерять доступ к интернету дети не говорят родителям о проблемах, а также могут начать использовать интернет вне дома и школы).
- 5** Будьте в курсе сетевой жизни вашего ребенка. Интересуйтесь его друзьями в интернете так же, как интересуетесь реальными друзьями.

КАК ЗАЩИТИТЬ ОТ ВРЕДНОЙ ИНФОРМАЦИИ РЕБЕНКА В ВОЗРАСТЕ 7–8 ЛЕТ

Эта памятка обеспечить информационную безопасность ребенка в возрасте 7–8 лет

В интернете ребенок старается посетить те или иные сайты, а возможно, и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования интернета, то есть Родительский контроль, или то, что вы сможете увидеть во временных файлах. В результате у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако родители будут по-прежнему знать, какие сайты посещает их ребенок.

Дети в этом возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах.

Советы по безопасному использованию интернета

- 1** Создайте домашние правила посещения интернета при участии ребенка и требуйте их выполнения.
- 2** Требуйте от ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что вы наблюдаете за ним не потому, что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
- 3** Компьютер с подключением к интернету должен находиться в общей комнате под присмотром родителей.
- 4** Используйте специальные детские поисковые машины.
- 5** Используйте средства блокирования нежелательного контента, как дополнение к стандартному Родительскому контролю.

Как защитить от вредной информации ребенка в возрасте 7–8 лет

Памятка для родителей

- 6** Создайте семейный электронный ящик, чтобы не позволить ребенку иметь собственный адрес.
- 7** Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
- 8** Приучите ребенка советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
- 9** Научите ребенка не загружать файлы, программы или музыку без вашего согласия.
- 10** Не разрешайте ребенку использовать службы мгновенного обмена сообщениями.
- 11** В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
- 12** Не забывайте беседовать с ребенком о его друзьях в интернете, как если бы речь шла о друзьях в реальной жизни.
- 13** Не делайте «табу» из вопросов половой жизни, так как в интернете ребенок может наткнуться на порнографию или сайты для взрослых.
- 14** Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Оставайтесь спокойными и напомните ребенку, что он в безопасности. Похвалите его и посоветуйте подойти еще раз в подобных случаях.