

ПАМЯТКА

для школьников

Как безопасно общаться 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 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 то, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить.
- 4** Не используй реальное имя. Когда в сети разговариваешь с незнакомыми людьми, не называй и не используй реальное имя. Не раскрывай информацию о себе: место жительства, место учебы и прочее.
- 5** Не сообщай свое местоположение. Избегай размещения фотографий в интернете, где ты изображен на местности, по которой можно определить местоположение.
- 6** Используй сложные пароли. При регистрации пиши сложные пароли. Они должны содержать не менее восьми знаков и включать в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак.
- 7** Используй разные пароли. Для социальной сети, почты и других сайтов создавай разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не ко всем сразу.

ПАМЯТКА

для школьников

Как безопасно пользоваться электронной почтой

Рекомендовано
Минобрнауки

- 1 Выбери правильный почтовый сервис.** В интернете много бесплатных. Однако почту лучше заводить на популярном сервисе, которым уже пользуются твои знакомые.
- 2 Не пиши о себе в адресе почты.** Не указывай в почтовом адресе личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2018@» вместо «андрей2005@».
- 3 Используй двухэтапную авторизацию.** Для двухэтапной авторизации помимо пароля нужно вводить код, который присыпают по СМС.
- 4 Выбери сложный пароль.** Для каждого почтового ящика должен быть свой сложный, устойчивый к взлому пароль.
- 5 Используй проверочный вопрос.** Придумай сам свой личный вопрос для идентификации, если сервис дает такую возможность.
- 6 Заведи несколько почтовых ящиков.** Первый для частной переписки с адресатами, которым ты доверяешь. Этот электронный адрес не нужно использовать при регистрации на форумах и сайтах.
- 7 Не открывай вложения писем.** Не открывай файлы и другие вложения в письмах, даже если они пришли от друзей. Уточни у них, отправляли ли они тебе эти файлы.
- 8 Выходите из почты.** Не забывай нажимать «Выйти» после окончания работы на почтовом сервисе, перед тем как закрыть вкладку с сайтом.

ПАМЯТКА

для школьников

Как защититься от кибербуллинга

Рекомендовано
Минобрнауки

КИБЕРБУЛЛИНГ – ситуация, когда человека в Сети преследуют сообщениями, которые содержат оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование.

- 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 оскорблением на оскорбления, то только еще больше разожжешь конфликт.
- 2** Управляй своей киберрепутацией. Ищи способы выяснить, кто стоит за анонимным аккаунтом обидчика. Анонимность в Сети мнимая.
- 3** Береги виртуальную честь смолоду. Не веди хулиганский образ виртуальной жизни. Интернет фиксирует все действия и сохраняет их. Удалить их будет сложно.
- 4** Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
- 5** Блокируй агрессора. В программах обмена мгновенными сообщениями, в социальных сетях можно запретить конкретным адресам присыпать сообщения.
- 6** Поддержи жертву кибербуллинга. Покажи преследователю, что оцениваешь его действия негативно. Сообщи взрослым о факте агрессивного поведения в Сети.

ПАМЯТКА

для школьников

Как защититься от компьютерных вирусов

Рекомендовано
Минобрнауки

КОМПЬЮТЕРНЫЙ ВИРУС – это программа, которая может создавать свои копии. Вирусы повреждают или уничтожают файлы на зараженном компьютере и всю операционную систему в целом. Чаще всего распространяются вирусы через интернет.

- 1** Загрузи современную операционную систему. Используй современные операционные системы с высоким уровнем защиты от вредоносных программ.
- 2** Обновляй операционную систему. Включи режим автоматического обновления операционной системы. Если в системе нет такого режима, регулярно устанавливай обновления самостоятельно. Загружай их с официального сайта разработчика.
- 3** Используй права пользователя. Работай на компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ автоматически установиться.
- 4** Не рискуй. Используй антивирусные программные продукты проверенных производителей с автоматическим обновлением баз.
- 5** Ограничь доступ к своему компьютеру. Не разрешай посторонним пользоваться своим компьютером.
- 6** Выбирай тщательно источники. Копируй и загружай файлы только с проверенных съемных носителей или интернет-ресурсов. Не открывай файлы, которые получил из ненадежных источников. Даже те, которые прислал твой знакомый. Уточни у него, отправлял ли он тебе их.

ПАМЯТКА

для школьников

Как безопасно пользоваться сетью Wi-Fi

Рекомендовано
Минобрнауки

Wi-Fi – это беспроводной способ передачи данных с помощью радиосигналов. В кафе, отелях, аэропортах часто можно бесплатно выйти в интернет через Wi-Fi. Но общедоступные сети Wi-Fi небезопасны.

- 1** Не передавай личную информацию через общедоступные сети Wi-Fi. Желательно не вводить пароли доступа, логины и номера.
- 2** Используй и обновляй антивирусные программы и брандмауэр. Так ты обезопасишь себя от закачки вируса на устройство.
- 3** Отключи функцию «Общий доступ к файлам и принтерам» при использовании Wi-Fi. Эта функция закрыта по умолчанию, однако некоторые пользователи активируют ее 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. То есть при наборе веб-адреса вводи именно «<https://>».
- 6** Отключи функцию «Подключение к Wi-Fi автоматически» в мобильном телефоне. Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

ПАМЯТКА

для школьников

Как безопасно расплачиваться электронными деньгами

Рекомендовано
Минобрнауки

ЭЛЕКТРОННЫЕ ДЕНЬГИ – это удобный способ платежей, однако за ними часто охотятся мошенники. В России закон разделяет электронные деньги на два вида – анонимные и персонализированные. Разница в том, что анонимные – это те, в которых разрешается проводить операции без идентификации пользователя, а в персонализированных идентификация пользователя обязательна.

- 1** **Привяжи к счету мобильный телефон.** Это самый удобный способ восстановить к нему доступ. Привязанный телефон поможет, если забудешь платежный пароль или зайдешь на сайт с незнакомого устройства.
- 2** **Используй одноразовые пароли.** После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля.
- 3** **Придумай сложный пароль.** Преступникам будет не просто угадать сложный пароль. Сложные пароли – это пароли, которые содержат не менее восьми знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак. Например, StROng!;:
- 4** **Береги личные данные.** Не вводи их на сайтах, которым не доверяешь.

ПАМЯТКА

для школьников

Как безопасно пользоваться смартфоном, планшетом

Рекомендовано
Минобрнауки

- 1** **Будь осторожен.** Когда тебе предлагают бесплатный контент, в нем могут быть скрыты платные услуги.
- 2** **Думай, прежде чем отправить СМС, фото или видео.** Ты точно знаешь, где они окажутся в конечном итоге?
- 3** **Обновляй операционную систему смартфона.** Это дополнительная защита.
- 4** **Используй антивирусные программы для смартфонов.** Регулярно обновляй их.
- 5** **Не загружай приложения от неизвестного источника.** Они могут содержать вредоносное программное обеспечение.
- 6** **Зайди в настройки браузера и удали cookies.** Сделай это сразу после того, как ты выйдешь с сайта, где вводил личную информацию.
- 7** **Проверяй платные услуги на твоем номере.** Иногда могут активировать новые.
- 8** **Не всем давай номер телефона.** Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь.
- 9** **Выключай Bluetooth, когда не используешь его.** Иногда проверяй, не забыл ли выключить.

ПАМЯТКА

для школьников

Как безопасно играть online

Рекомендовано
Минобрнауки

ONLINE-ИГРЫ объединяют людей по всему миру. Игроки покупают диск, оплачивают абонемент или дополнительные опции. На эти средства совершаются системы авторизации, закрываются уязвимости. В играх стоит опасаться кражи пароля.

- 1** **Блокируй неадекватов.** Заблокируй в списке игроков того, кто ведет себя агрессивно по отношению к тебе или создает неприятности.
- 2** **Пожалуйся администраторам игры на поведение агрессивного игрока.** Желательно приложить доказательства в виде скринов.
- 3** **Будь осторожен.** Не указывай личную информацию в профайле игры.
- 4** **Следи за своим поведением.** Уважай других участников игры.
- 5** **Устанавливай проверенные утилиты.** Избегай неофициальных патчей и модов.
- 6** **Берегись от взлома.** Используй сложные и разные пароли.
- 7** **Не отключай антивирус во время игры.** Пока ты играешь, твой компьютер могут заразить.

ПАМЯТКА

для школьников

Как защититься от фишинга

Рекомендовано
Минобрнауки

ФИШИНГ (от английского слова fishing – рыбная ловля) – вид интернет-мошенничества. Его главная цель – получить конфиденциальные данные пользователей – логины и пароли.

- 1 Следи за своим аккаунтом.** Если подозреваешь, что аккаунт взломали, нужно заблокировать его и сообщить администраторам ресурса об этом как можно скорее.
- 2 Посещай только безопасные веб-сайты.** В их числе – сайты интернет-магазинов и поисковых систем.
- 3 Используй сложные и разные пароли.** Если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в Сети, а не ко всем.
- 4 Предупреди всех своих знакомых, которые добавлены у тебя в друзья, если тебя взломали.** От твоего имени могут рассыпать спам и ссылки на фишинговые сайты.
- 5 Спрячь данные.** Установи надежный пароль (PIN) на мобильный телефон.
- 6 Отключи сохранение пароля в браузере.** Сохраненные пароли крадут чаще.
- 7 Не открывай файлы и другие вложения в письмах.** Даже если они пришли от твоих друзей. Уточни у них, отправляли ли они тебе эти файлы.

ПАМЯТКА

для школьников

Как защитить свою цифровую репутацию

Рекомендовано
Минобрнауки

ЦИФРОВАЯ РЕПУТАЦИЯ – это твой имидж, который формируется из информации о тебе в интернете. Компрометирующая информация в интернете может серьезно отразиться на реальной жизни. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в Сети.

Многие подростки легкомысленно относятся к публикации личной информации в интернете, не понимая возможных последствий. Ты даже не задумываешься о том, что фотография, размещенная пять лет назад, может стать причиной отказа принять тебя на работу.

Комментарии, фотографии и твои действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред.

СОВЕТЫ ПО ЗАЩИТЕ ЦИФРОВОЙ РЕПУТАЦИИ:

- 1** Не публикуй сразу. Подумай, прежде чем что-то публиковать у себя в блоге или в социальной сети, пересыпал в личном сообщении.
- 2** Установи ограничения в настройках профиля. Ограничь просмотр профиля и его содержимого. Сделай его только «для друзей».
- 3** Берегись исков за оскорбление личности в интернете (ст. 282 УК). Не размещай информацию, которая может кого-то обижать, и не ссылайся на нее.

ПАМЯТКА

для школьников

Что такое авторское право



Чтобы использовать возможности цифрового мира, нужно соблюдать права 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, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность – на произведения науки, литературы и искусства. Авторские права выступают как гарантия возможностей автора заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать или размещать в интернете.

«Пиратское» программное обеспечение несет в себе многие риски: от потери данных до блокировки устройства, где установлена нелегальная программа. Не забывайте, что в Сети можно найти легальные и бесплатные программы со сходным функционалом.

ПАМЯТКА

для родителей

Как защитить от вредной информации ребенка в возрасте 9–12 лет



В этом возрасте дети уже многое знают об интернете. Совершенно正常но, что они хотят что-то увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

- 1 Договоритесь о правилах.** Создайте домашние правила посещения интернета при участии ребенка и требуйте их выполнения.
- 2 Ограничьте время в Сети.** Требуйте от ребенка соблюдения временных норм нахождения за компьютером.
- 3 Наблюдайте за ребенком.** Смотрите, что делает ваш ребенок при работе за компьютером. Покажите ему, что вы беспокоитесь о его безопасности и всегда готовы помочь ему.
- 4 Поставьте компьютер в общую комнату.** Так при работе на компьютере ребенок будет находиться под присмотром, когда использует интернет.
- 5 Пользуйтесь фильтрами контента.** Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- 6 Спрашивайте о друзьях в Сети.** Не забывайте принимать непосредственное участие в жизни ребенка, беседовать о его друзьях в интернете.

- 7** **Запретите личные встречи.** Настаивайте, чтобы ребенок никогда не соглашался на личные встречи с друзьями по интернету.
- 8** **Создайте список сайтов.** Позволяйте ребенку заходить только на сайты из «белого» списка, который создадите вместе с ребенком.
- 9** **Обсудите использование личной информации в Сети.** Приучите ребенка никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в интернете.
- 10** **Ограничьте возможность загрузки программ.** Приучите ребенка не загружать программы без вашего разрешения. Объясните ему, что он может случайно загрузить вирусы или другое нежелательное программное обеспечение. Создайте ребенку ограниченную учетную запись для работы на компьютере.
- 12** **Договоритесь сообщать об угрозах.** Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Напомните ребенку, что он в безопасности.
- 13** **Поговорите о порнографии.** Расскажите ребенку о порнографии в интернете.
- 14** **Получите доступ к почте.** Настаивайте на том, чтобы ребенок предоставлял вам доступ к своей электронной почте, чтобы вы убедились, что он не общается с незнакомцами.
- 15** **Расскажите об ответственности за хулиганство в Сети.** Объясните ребенку, что нельзя в интернете хулиганить, распространять сплетни или угрожать.

ПАМЯТКА

для родителей

Как защитить от вредной информации ребенка в возрасте 13–17 лет

Рекомендовано
Минобрнауки

- 1** Договоритесь о правилах. Создайте домашние правила посещения интернета при участии ребенка и требуйте их безусловного выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в интернете, руководство по общению в интернете (в том числе в чатах).
- 2** Поставьте компьютер в общую комнату. Компьютер с подключением к интернету должен находиться в общей комнате.
- 3** Спрашивайте о друзьях в Сети. Не забывайте беседовать с ребенком о его друзьях в интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми ребенок общается сообщениями через мессенджеры, чтобы убедиться, что эти люди вам знакомы.
- 4** Пользуйтесь фильтрами контента. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
- 5** Следите за программами для общения. Необходимо знать, какими чатами пользуется ребенок. Советуйте использовать чаты, которые модерируют. Настраивайте их так, чтобы ребенок не общался в приватном режиме.
- 6** Запретите личные встречи. Настаивайте на том, чтобы ребенок один никогда не встречался лично с друзьями из интернета.

- 7** **Обсудите использование личной информации в Сети.** Приучите ребенка не выдавать свою личную информацию через электронную почту, чаты, мессенджеры, регистрационные формы, личные профили и при регистрации на конкурсы в интернете.
- 8** **Ограничьте возможность загрузки программ.** Приучите ребенка не загружать программы без вашего разрешения. Объясните ему, что он может случайно загрузить вирусы или другие нежелательные программы.
- 9** **Договоритесь сообщать об угрозах.** Приучите ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом. Напомните ребенку, что он в безопасности. Похвалите его и посоветуйте подойти еще раз в подобных случаях.
- 10** **Поговорите о порнографии.** Расскажите ребенку о порнографии в интернете. Помогите ему защититься от спама, в том числе с порнографическим содержанием.
- 11** **Договоритесь об осторожности в Сети.** Научите ребенка не выдавать в интернете свой реальный электронный адрес, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- 12** **Просматривайте сайты.** Приучите себя знакомиться с сайтами, которые посещает ребенок.
- 13** **Научите ребенка уважать других в интернете.** Убедитесь, что он знает о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.
- 14** **Расскажите об ответственности за хулиганство в сети.** Объясните ребенку, что нельзя использовать интернет для хулиганства, распространения сплетен или угроз другим людям.
- 15** **Поговорите об азартных играх.** Обсудите с ребенком проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

ПАМЯТКА

для родителей

Как обеспечить информационную безопасность ребенка. Общие правила

Рекомендовано
Минобрнауки

- 1** Ваше внимание к ребенку – главный метод защиты. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него.
- 2** Внимательно изучите связанные аккаунты в социальных сервисах, где есть аккаунт ребенка. Это [vkontakte.ru](#), [blogs.mail.ru](#) и др. Смотрите, что размещают группы и люди, на которых он подписан, включая фото и видео.
- 3** Проверьте, с какими другими сайтами связан социальный сервис вашего ребенка. Страницы вашего ребенка могут быть безопасными, но при этом 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. Не реагируйте слишком остро, 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.