1. Тема: «Мое сетевое Я»

Содержание работы: Правила ведения аккаунта в соц. сетях (цифровой след), сетевой этикет.

Основной материал для занятия

Социальная сеть — платформа, веб-сайт, предназначенный для построения и организации общения и социальных отношений в сети Интернет. Наиболее популярными социальными сетями являются ВКонтакте, Одноклассники, Facebook, Twitter, Instagram, TikTok. Социальная сеть позволяет зарегистрированным участникам выражать свои мысли и чувства, а также больше узнавать о других пользователях. Так дети могут найти сверстников, которых они встречают в школе, на улице и завести с ними знакомства и дружбу. В социальных сетях размещается много различной информации: персональные данные ребенка, родителей, родных и друзей; различный контент (информация) с рекламами, новостями и просто информационными блоками; различные лицензионные и «пиратские» аудио-, видеофайлы; группы и сообщества любых направлений и др.

Общение в сети представляет собой почти реальное общение, однако оно заменяет саму манеру взаимодействия на использование коротких, но емких выражений, картинок и символов. При общении в сети с помощью коротких фраз, сжатых выражений, обозначающих эмоции картинками-смайликами, выработался особый язык, построенный на графических символах и словах со специально искаженными орфографическими и лексическими нормами. Общение в сети можно назвать торопливым и предельно упрощенным. При помощи знаков препинания эмоции выражаются по-разному.

Общение в социальных сетях имеет свои специфические особенности, которые отличаются от привычного очного разговора. Среди этих особенностей можно отметить следующие:

– Анонимность. Несмотря на то, что иногда возможно получить некоторые сведения из анкет и даже фотографию собеседника, они недостаточны для реального и более или менее адекватного восприятия личности. Кроме того, в сети часто принято укрывание или презентация ложных сведений. Человек в сети может проявлять и проявляет большую свободу высказываний, так как риск разоблачения и отрицательной личной оценки окружающими минимален.

– Своеобразие межличностного восприятия в условиях отсутствия невербальной информации.

– Добровольность и желательность контактов. Пользователь добровольно завязывает контакты или уходит от них, а также имеет право прервать их в любой момент.

– Затрудненность эмоциональной части общения и, в то же время, стремление к эмоциональному наполнению текста, которое выражается в создании специальных значков для обозначения эмоций или в описании эмоций словами (в скобках после основного текста послания).

– Стремление к нетипичному поведению. Часто пользователи показывают себя с иной стороны, чем в условиях реальной социальной нормы.

Можно заметить гонку подростков за количеством онлайн-друзей. Но к чему приводит неразборчивость в контактах, безответственность и сомнительная осведомленность о настройках профилей? Как показывает практика, многие подростки не знают последствия чрезмерной открытости, не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями. Совокупность всех данных о пользователе называют «цифровой тенью», электронным двойником реального человека. Чем больше мы пишем о себе в сети Интернет, чем больше размещаем фото и ссылок, ставим «лайк» под понравившимся постом, тем больше знают о нас потенциальные мошенники. Поэтому, прежде всего нужно понять, всем ли будет доступна информация о Вас в социальных сетях и с кем Вы готовы делиться своими планами, событиями и фотографиями. Личная информация, которую Вы размещаете в Интернете, может попасть в руки мошенникам, после чего у них открываются широкие возможности для совершения неправомерных действий: рассылка спама среди друзей того пользователя, у которого взломали аккаунт, а также распространение среди них коммерческой или иной информации и т.п.

Чтобы не попадать в такие неприятные ситуации, каждому пользователю социальных сетей нужно серьезно подумать о том, как защитить свой аккаунт от взлома и соблюдать правила безопасности в социальных сетях.

Правила безопасного общения в социальных сетях

1. При регистрации в социальной сети необходимо использовать оригинальные и сложные пароли, состоящие из разных регистров букв и цифр, с количеством знаков не менее. Использование уникального пароля для каждого отдельного аккаунта является важным условием для повышения защищенности пользователя. Например, пароль от вашего аккаунта в социальной сети и пароль от электронной почты не должны совпадать. Для еще больше защищенности аккаунта рекомендуется включить двухфакторную аутентификацию, которая, наряду с паролем, в качестве первого фактора известного только самому пользователю, требует ввода второго фактора в виде уникального кода, владельцем которого является тоже пользователь. Код генерируется либо провайдером онлайн услуги либо специальным приложением установленным на мобильное устройство пользователя. Получить код от провайдера можно по СМС или с помощью голосового вызова. В любом случае, сгенерированный код имеет срок годности или определенную продолжительность службы.

2. Не следует публиковать свои личные данные: пароли, телефоны, адреса, дату рождения и другую личную информацию. Обязательно выходите из аккаунтов после завершения работы.

3. Используйте настройки конфиденциальности аккаунта. Так незнакомые люди не увидят Вашу личную информацию. Не сообщайте данные аккаунта друзьям и знакомым. Если заходите в социальную сеть или почту с чужого компьютера, не забудьте выйти.

4. Необходимо ограничить список друзей: в друзьях не должно быть случайных и незнакомых людей. Общаясь в социальных сетях, не следует доверять всем, кто захочет установить с вами контакт. Особенно если в разговоре появляются просьбы, связанные с отправкой SMS на какой-либо номер или отправки внезапно пришедших на телефон кодов.

5. Устанавливайте антивирусные программы, только надежная защита на компьютере (или ином устройстве) минимизирует риск взлома странички в социальной сети.

6. Никогда не открывайте подозрительные сообщения, в которых находятся ссылки на неизвестные ресурсы, и никогда не переходите по этим ссылкам, не устанавливайте неизвестные программы. Безопасность всей информации на компьютере зависит не только от антивируса, но еще больше она зависит именно от действий пользователя. Иногда сообщения, отправленные вам якобы вашими друзьями, могут быть отправлены злоумышленниками, которые взломали их аккаунты. При открытии подобных сообщений может быть запущена вредоносная программа, записывающая пароли. Поэтому если сообщение кажется вам подозрительным или содержит подозрительную ссылку, свяжитесь с другом напрямую или по телефону, чтобы убедиться, что сообщение действительно пришло от него.

7. Не устанавливайте приложения для социальных сетей, которые по описанию позволяют скачать музыку, видео и другое, если вы не уверены в безопасности этих приложений. Часто при установке они запрашивают логин и пароль от вашего аккаунта – все это способы работы злоумышленников, которые пытаются заполучить доступ к вашему аккаунту.

8. Не пересылайте конфиденциальную информацию (номер банковской карты, ПИН-код, паспортные данные) через сообщения социальных сетей. Письма со сканами документов лучше удалять сразу после отправки или получения, не надо хранить их в почте.

9. Если Вы действительно хотите встретиться с человеком, с которым познакомились в интернете, то договоритесь о встрече в общественном месте, и желательно взять с собой кого-то еще, например, друга. Если сетевой друг считает, что присутствие кого-то еще плохая идея, то стоит отказаться от встречи.

10. Во время общения в сети с другими пользователями игнорируйте их плохое поведение, воздержитесь от ответа на провокационные сообщения. Как и в реальной жизни, существуют люди, которые по разным причинам ведут себя агрессивно, оскорбительно или провокационно по отношению к другим или хотят распространить вредоносный контент. Обычно лучше всего игнорировать и затем заблокировать таких пользователей.

С каждым годом молодежи в интернете становиться все больше, среди них школьники - самые активные пользователи Интернета. Бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в сеть. Но, как известно, общедоступные Wi-Fi сети не являются полностью безопасными. ,

Основные советы по безопасному использованию сети Wi-Fi

1. Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и другие личные номера.

2. Используйте и обновляйте антивирусные программы. Тем самым вы обезопасите себя от закачки вируса на свое устройство.

3. При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют ее для удобства использования в работе или учебе.

4. Не используйте публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту.

5. Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://».

6. В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускайте автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

Большая часть школьников уверена, что при совершении того или иного действия в сети они останутся неизвестными. В сети Интернет сейчас достаточно инструментов и инструкций по созданию противоправного контента, вирусов, фальсификации страниц известных социальных сетей. Подросток, пользуясь такими инструкциями, может преступить закон, и в таком случае от его «анонимности» не останется и следа. Если первым аспектом вопроса является безопасность персональных данных, то вторым – противоправный и негативный контент. Размещение подростками личных фотографий является попыткой самовыражения, вместе с тем они хотят получить оценку окружающих. Такие фотографии имеют провокационный характер и дают злоумышленникам доступ к большому спектру персональных данных. Помните, что все совершаемые в сети действия оставляют след. Та его часть, в которой есть персональные данные в любом виде, называется «цифровым следом» конкретного человека. По такому следу можно вычислить Ваш маршрут, где и когда Вы бываете, что покупаете, с кем общаетесь и т.п. Подобная информация может быть опасна, если ее используют злоумышленники.

Помимо опасности разоблачения, доверия к незнакомцам и потери персональных данных и анонимности в сети есть еще одна опасность – неправильное общение с собеседниками. Это может быть спровоцированная агрессия, неграмотная письменная речь, слишком смелые высказывания и т.п. Разберемся, как правильно общаться в социальных сетях. Правила общения в сети называют сетевым этикетом. Наряду с обычным этикетом эти правила необходимо соблюдать, чтобы не провоцировать скандалы и агрессию, не обидеть собеседника и произвести хорошее впечатление на тех, с кем идет переписка.

Чего нельзя делать в сети Интернет?

Прежде всего нельзя делать тех вещей, которые не поощряются в любом цивилизованном обществе:

- употреблять ненормативную лексику;
- оскорблять людей;
- воровать;
- умышленно пытаться что-то сломать;
- отправлять инструкции, объясняющие, как совершить незаконные действия, а также спрашивать о возможных способах совершения такого рода действий;
- публиковать личные письма без согласия их авторов;
- затевать или продолжать дискуссию на любую тему в местах (конференции, форумы и т.п.), не предназначенных для этого.

При общении в сети используют некоторые специальные термины

Оверквотинг (overquoting) - избыточное цитирование. Как правило, когда пользователь отвечает на чье-либо письмо, исходный текст письма сначала цитируется (при этом он визуально выделяется отступом или другим шрифтом), а затем уже идет сам ответ. Это делается для того, чтобы остальные присутствующие поняли, что, собственно, комментируется. Самой распространенной ошибкой в этом случае является так называемый оверквотинг. Потому что для того, чтобы был понятен ответ, почти всегда ни к чему цитировать все исходное письмо. Достаточно процитировать только ту часть, которая необходима для понимания ответа.

Флеймы (flames) - это эмоциональные замечания, часто высказанные без учета мнения других участников разговора. Это сообщения, где такт - не самое главное, а цель - вызвать реакцию пользователей. Флейм - это «спор ради спора». Крайняя степень флейма проявляется в случае, когда все забывают, из-за чего начался разговор и начинают ожесточенно ругаться друг с другом. Мы говорим про человека, что он разжигает флейм, если он:

- Переходит по ходу разговора на личности
- Допускает оскорбления личного, национального, религиозного или профессионального характера
- Ведет спор неуравновешенно
- Провоцирует скандал

Есть простое правило - никогда не стоит поддерживать флейм. Игнорируйте «флеймеров» - и тогда вас, несомненно, начнут уважать все остальные.

Флуд - это поток сообщений, не несущих почти никакой смысловой нагрузки. Это такие сообщения, которые можно было бы удалить (а точнее, не писать) без всякого ущерба

для сообщества. Обычно «флудят» пользователи, которым по большому счету нечего сказать, но которые хотят привлечь к себе внимание. Они начинают отвечать почти на каждое сообщение, причем ответы не несут никакой смысловой нагрузки и выглядят как короткие однострочные сообщения. «Флуда» следует избегать. Он замедляет загрузку страниц, увеличивает количество ненужной информации, раздражает других пользователей.

Правила «сетевого этикета»

1. Помните, что Вы говорите с человеком.

Не делайте другим того, чего не хотите получить от них сами. Поставьте себя на место человека, с которым говорите. Отстаивайте свою точку зрения, но не оскорбляйте окружающих. Когда Вы используете Интернет, то имеете дело с экраном компьютера. Вы не можете жестикулировать, изменять тон, и выражение Вашего лица не играет никакой роли.

Когда Вы ведете разговор - по электронной почте или в социальной сети - можно легко ошибиться в толковании слов Вашего собеседника. И, к сожалению, забыть о том, что Ваш адресат тоже человек со своими чувствами и привычками. Однако не забывайте о главном принципе сетевого этикета: везде в Сети находятся реальные люди.

И еще одна причина, по которой следует быть вежливым в Сети. Когда Вы связываетесь с кем-либо в киберпространстве, помните, что Ваши слова фиксируются. Возможно, они сохранятся там, куда Вы уже не сможете добраться. Иными словами, есть шанс, что они еще вернутся и навредят Вам. И у Вас нет никакой возможности повлиять на этот процесс.

2. Придерживайтесь тех же стандартов поведения, что и в реальной жизни.

В реальной жизни большинство из нас подчиняется законам, иногда из-за ограничений, иногда из-за опасений быть пойманным. В виртуальном пространстве шансы быть пойманным - сравнительно невелики. Люди иногда забывают о том, что «за экраном» находится живой человек, и думают, что в Сети правила поведения не так строги, как в обычной жизни.

Это заблуждение объяснимо, но все равно - это заблуждение. Стандарты поведения могут отличаться в разных точках виртуального пространства, однако, они не более гибкие, чем в реальной жизни.

Соблюдайте этику общения. Не верьте тому, кто говорит «Вся этика здесь заключается в том, что Вы сами для себя установите». Если Вы встречаетесь с проблемой этического характера в киберпространстве, подумайте, как бы Вы поступили в реальной жизни. Скорее всего, Вы быстро найдете решение.

3. Помните, где Вы находитесь в киберпространстве.

То, что без колебаний принимается в одном месте, могут посчитать за грубость в другом. Оказавшись в новой области виртуального пространства, сначала осмотритесь. Потратьте время на изучение обстановки - почитайте, как и о чем говорят люди. После этого вступайте в разговор.

4. Уважайте время и возможности других.

Когда Вы посылаете электронную почту или отправляете сообщение в сети, Вы фактически претендуете на чье-то время. И тогда Вы отвечаете за то, чтобы адресат не потратил это время зря.

Понятие «возможности» включает в себя пропускную способность канала, по которому происходит связь и физическую емкость носителей информации на удаленном компьютере. И если Вы случайно отправили в одно и то же видео или фото в пять одинаковых сообщений, Вы потратили как время подписчиков, так и возможности системы (ведь Вы занимали линию передачи и место на диске).

У людей не так много времени для чтения сообщений, учитывая количество последних. Прежде, чем Вы отправите свое письмо, подумайте, действительно ли получатели нуждаются в нем. Если Вы ответите себе «нет», лучше не тратить их (и свое) время. Если же Вы сомневаетесь, подумайте дважды прежде, чем отправить сообщение.

5. Сохраняйте «лицо».

Используйте преимущества анонимности. В Сети (например, в конференциях) Вы можете встретиться с теми, кого никогда бы не встретили в реальной жизни и никто не осудит Вас за цвет кожи, глаз, волос, за Ваш вес, возраст или манеру одеваться. Однако Вас будут оценивать по тому, как Вы пишете. Для тех, кто находится в Сети, это имеет значение. Таким образом, правила грамматики играют важную роль. Отдавайте себе отчет в том, что пишете.

Осмысливайте содержание Вашего письма. Когда Вы хотите сказать, что-то вроде «мне кажется...» или «я слышал, что...», спросите себя - а не проверить ли еще раз правильность Ваших фактов. Недостоверная информация способна вызвать целый шквал эмоций в Сети. И если это повторяется второй и третий раз, может произойти, как в игре «испорченный телефон»: ваши слова будут искажены до неузнаваемости.

Кроме того, убедитесь, что Ваши послания ясны и логически выдержанны. Можно сочинить параграф текста, который будет безукоризненным с точки зрения грамматики, но совершенно бессмысленным. Это часто случается, если Вы хотите убедить кого-либо в Вашей правоте, используя множество сложных и длинных слов, которые Вам самому не очень-то и знакомы. Не оскорбляйте пользователей. Наконец, будьте терпеливы и вежливы. Не употребляйте ненормативную лексику, не идите на конфликт ради самого конфликта.

6. Помогайте другим там, где Вы это можете делать.

Почему задавать вопросы в виртуальном пространстве эффективно? Потому что Ваши вопросы читают многие люди, знающие на них ответ. И даже если квалифицированно ответят только несколько человек, общий объем знаний в Сети увеличится. Интернет сам по себе «вырос» из стремления ученых к обмену опытом. Постепенно в этот увлекательный процесс втянулись другие пользователи. Обмен опытом - увлекательное занятие. Это старая и хорошая традиция сети Интернет.

7. Не ввязывайтесь в конфликты и не допускайте их.

Запрещает ли сетевой этикет флеймы? Не совсем. Флеймы - тоже старая традиция Сети. Флеймы могут доставлять удовольствие, как сочинителям, так и читателям. Но сетевой этикет против флеймов, перерастающих в серии злобных посланий, которыми обмениваются, как правило, два или три участника дискуссии. Такие «войны» могут буквально захватить переписку и разрушить дружескую обстановку.

8. Уважайте право на частную переписку.

9. Не злоупотребляйте своими возможностями.

Некоторые люди в виртуальном пространстве чувствуют себя профессионалами. Это асы в каждой сетевой игре, эксперты в каждом офисе и системные администраторы. Обладая более широкими знаниями или имея в руках более широкие полномочия, эти люди автоматически получают преимущество. Однако это не означает, что они могут им пользоваться. Например, системные администраторы не должны читать частные почтовые сообщения.

10. Учитесь прощать другим их ошибки.

Каждый когда-то был новичком. Поэтому когда кто-то допускает ошибку - будь это опечатка в слове, неосторожное послание, глупый вопрос или неоправданно длинный ответ - будьте к этому снисходительны. Даже если очень хочется ответить, подумайте дважды. Если Вы обладаете хорошими манерами, это еще не значит, что Вы имеете право на преподавание этих манер всем остальным.

Если же Вы решили обратить внимание пользователя на его ошибку, сделайте это корректно и лучше не в общем чате, а в частном письме. Как известно, исправления в тексте часто содержат грамматические ошибки; также и указание на несоблюдение правил этикета, бывает, демонстрирует нарушение этого же этикета.

Дополнительный материал

При выборе пароля не следует использовать:

- ☒ стандартные комбинации букв и цифр, такие как 123456, qwerty, qwerty1234, 1q2w3e4r5t6y.
- ☒ комбинации номеров телефона, адресов, дат рождений и другой личной информации;
- ☒ последовательные строки из повторяющихся букв или цифр;
- ☒ части имени пользователя с добавлением цифр, или имена родственников;
- ☒ слова из словаря и географические названия.

Правила создания оригинальных и сложных паролей

- ☑ Старайтесь использовать буквы разного регистра, а также цифры, в количестве символов от 6-8.
- ☑ Старайтесь не использовать подряд идущие символы, использовать как можно меньше одинаковых букв и символов в целом.
- ☑ В идеале пароль должен представлять из себя фразу или слово без повторяющихся букв, несколькими заглавными буквами и цифрами.
- ☑ Для лучшего запоминания в качестве ключевых слов можно использовать названия любимых книг, групп или авторов.