KASPERSKY lab

Безопасное использование соцсетей и общение за их пределами для учащихся средних классов

Материал для учителя

KASPERSKY lab

Безопасное использование соцсетей и общение за их пределами для учащихся средних классов

Определение социальной сети звучит следующим образом: **Социальная сеть** – платформа, онлайн-сервис и веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений в Интернете. Проще говоря, это то, что позволяет людям общаться в интернете. Общение в социальных сетях не ограничивается личными разговорами, а в значительной мере похоже на реальную жизнь: люди общаются здесь и один на один, и группами, создают «кружки» по интересам. В то же время общение в социальной сети значительно заметнее для окружающих, чем общение в реальной жизни, так как большая его часть происходит у всех на глазах, а кроме общения в группах или один на один есть возможность размещать «контент»: фотографии, видео, музыку, картинки, которые могут посмотреть все, у кого есть доступ к твоему аккаунту или к группе, где ты их разместил.

Задание. Какие социальные сети вы знаете?

Мессенджеры по сути являются подвидом социальных сетей. Изначально они появились как программы мгновенного обмена сообщениями между двумя людьми. Затем в них появилась возможность создавать группы – чаты, в которых могут участвовать только твои друзья, а могут сотни незнакомых друг другу людей. Еще один формат общения в мессенджерах – каналы, в которых один человек, зачастую инкогнито, пишет о том, что интересно ему и его подписчикам.

Задание. Какие мессенджеры вы знаете?

Задание. Каждый человек пользуется более чем одной социальной сетью. Сейчас вы видите логотипы разных соцсетей. Знаете ли вы их все? Впишите их названия, начиная с верхнего левого угла и заканчивая правым нижним. Отметьте галочкой те из них, которыми вы пользуетесь. В рабочих листах впишите также те соцсети и мессенджеры, которых нет в этом списке, но которыми вы пользуетесь.

Дополнительные данные для учителя: Самые популярные соцсети в России среди детей и подростков – это Вконтакте и Instagram, некоторые ребята используют также Twitter и Facebook. Среди мессенджеров наиболее популярны мессенджер Вконтакте, Whatsapp и Telegram. Кроме того, большинство подростков так или иначе использует Youtube – для просмотра разрозненных видео, подписки на каналы определенных видеоблогеров или для самостоятельного ведения каналов. Популярна среди подростков и игровая платформа Steam, сочетающая в себе магазин игр и социальную сеть. Средний возраст вхождения в соцсети в России – 8 лет, несмотря на то, что пользовательские соглашения большинства из них допускают использование соцсети лицами, достигшими 13 или более лет.

Задание. Подумайте, есть ли какие-то риски в социальных сетях? Что плохого может там произойти? Приведите 2–3 примера.

Для социальных сетей актуальны все те же самые риски, что и для всего интернета: здесь может распространяться назойливый спам, содержащий вредоносный код, мошенничество, рекламу. Кроме «виртуальных» угроз для социальных сетей характерны и угрозы, аналогичные тем, с которыми мы встречаемся в реальной жизни, ведь здесь общается большое количество людей с разными целями, замыслами и устремлениями.

Итак, спам в соцсетях и мессенджерах процветает не меньше, чем в электронной почте. Спам – это рассылки, на которые вы не подписывались, но в социальных сетях под определение спама уже можно подвести и назойливую рекламу в пабликах.

Задание. Подумайте, какие спамерские сообщения вы встречали в социальных сетях или мессенджерах? Приведите 2–3 разных примера.

Спам в соцсетях бывает разный:

- Он может рекламировать различные товары. Некоторые из них просто вам совершенно не нужны, другие могут оказаться некачественными. Такие сообщения могут встречаться как среди личных сообщений, так и в лентах пабликов. Нередко такие рекламные сообщения распространяются в мессенджерах.
- Зачастую среди личных сообщений как в соцсетях, так и в мессенджерах вы можете увидеть сообщения от собственных друзей, которые ни с того ни с сего просят вас прислать им денег или перейти по ссылке, чтобы проголосовать за них в конкурсе. Это обман. Деньги отправятся совершенно не вашему другу, а по ссылке будет вредоносный код.
- В лентах пабликов нередко встречается реклама других пабликов. При этом совсем не обязательно, что рекламируемый паблик хотя бы капельку близок по тематике к тому, на котором размещается реклама. Более того, зачастую таким образом распространяются ссылки на неприличные группы или группы, содержащие неприятные снимки и видео.
- Недостоверная информация, специально распространяемая в соцсетях, тоже в определенном смысле является подвидом спама. Важно не верить с первого взгляда всему, что читаешь в социальной сети, поддельные новости могут распространяться так же, как и рекламные посты – администрации паблика просто платят деньги за ее размещение. Если вас заинтересовала какая-то новость, поищите информацию о ней в других источниках и постарайтесь убедиться, что это не обман.

Задание. Ответьте, можно ли знакомиться с новыми людьми в соцсетях, и объясните свой ответ.

Дополнительные данные для учителя: согласно результатам опросов, около 90% школьников получают предложения о дружбе в социальных сетях от незнакомых людей, более половины подростков в возрасте от 12 до 16 лет знакомится в социальных сетях с новыми людьми, а почти половина готовы пойти на встречу с виртуальным знакомым или уже были на таких встречах.

Задание. Ответьте, что делать, если незнакомый взрослый человек попытается заговорить с вами на улице, и объясните почему.

Общение с незнакомцами, тем более через социальные сети, не может быть безопасным. Если на улице к тебе подходит незнакомый человек и пытается заговорить, то ты, вероятнее всего, не станешь отвечать. Но на улице ты, по крайней мере, видишь, с кем общаешься. Можешь оценить его возраст и пол, а следовательно составить хотя бы какое-то понимание о том, с кем имеешь дело. В Интернете кто угодно может представиться кем угодно, и ты можешь не узнать правды, даже общаясь с человеком несколько лет.

Ни в коем случае нельзя принимать приглашения в друзья в соцсетях от незнакомых людей или начинать переписку в мессенджерах непонятно с кем. Нельзя пользоваться и приложениями для знакомств, позволяющими общаться со случайным пользователем, и тем более отправлять этому пользователю видео или фото.

Единственное исключение из этого правила – знакомства, которые могли бы случиться в реальности. К примеру, кто-то из ваших друзей хочет познакомить вас со своими бывшими одноклассниками из старой школы. Если до изобретения социальных сетей вам пришлось бы всем встретиться в каком-то реальном месте, то теперь такое знакомство может произойти и онлайн. Самое важное, что кто-то, кого вы хорошо знаете лично, хорошо знает людей, с которыми вас знакомит.

Задание. Посмотрите на картинку. Знаете ли вы, кто на ней изображен и из какого мультфильма этот кадр? Сможете ли вы предположить, что такое кибербуллинг, используя эту картинку?

Кибербуллинг – это травля в интернете. Тех, кто ею занимается, называет троллями. Обычно кибербуллингом называют назойливую травлю, которая повторяется и продолжается долгое время, но в последнее время любые нападки в сети могут попасть под это определение.

О кибербуллинге важно помнить две вещи:

1. Никогда не начинайте и не участвуйте в травле сами. Даже один неприятный комментарий может обидеть и оскорбить человека. Тем более неприятно может быть, если такие комментарии оставит много людей или если они повторяются. Когда вы хотите написать о человеке что-то неприятное, подумайте, хотели бы вы сами прочитать что-то подобное о себе.

2. Вы должны помнить, что ничто не делает вас исключительным и защищенным от травли. Жертвой травли может стать абсолютно любой человек, поскольку травля может начаться из-за одной единственной неудачной фразы или фотографии, ее может начать кто-то, кто завидует тебе или почему-то не любит тебя. То, что ты стал жертвой травли, не значит, что ты плохой; это значит, что тем, кто тебя травит, не хватает воспитания, чтобы нормально вести себя в сети.

Если ты стал жертвой травли, соблюдай следующие правила:

- Никогда не отвечай троллям, это только раззадорит их.
- Расскажи своим родителям и близким друзьям, но ни в коем случае не проси их вступиться за тебя – это еще хуже, чем отвечать самому. Если ты будешь проводить с ними больше времени и ощущать их поддержку, это поможет сгладить переживания из-за травли.
- Заблокируй обидчиков с помощью настроек социальной сети, если травля становится навязчивой.

Кстати о настройках. Знаете ли вы, что у всех социальных сетей и мессенджеров есть настройки?

Задание. Знаете ли вы, что можно в них настроить? Перечислите хотя бы 5 вещей, которые можно настроить или ограничить.

Задание. Что такое приватность?

Приватность имеет множество различных довольно сложных определений. Проще всего описать «приватность» как систему допусков разных людей к тем или иным данным о конкретном человеке, которую этот человек определяет сам. Настройки приватности в социальной сети как раз и определяют, какие данные и способы взаимодействия с вами вы оставляете доступными разным людям. Исходя из того, что общаться в социальной сети безопасно только с теми, кого знаешь лично, все возможные настройки приватности должны ограничиваться пунктом «только друзья». Кто может присылать мне личные сообщения? Только друзья. Кто может просматривать мою страницу? Только друзья. Если говорить об отсылке вам заявок на добавление в друзья, то это может делать кто угодно, иначе вы можете остаться вовсе без друзей. Но вы сами должны понимать, что принять такую заявку можно только от человека, которого вы знаете лично. Некоторые школьники в погоне за «лайками», в том числе и от незнакомых людей, оставляют незнакомцам возможность просматривать свою страницу, считая, что если в остальном приватность настроена достаточно строго и незнакомцы видят только снимки или статусы, которые могут лайкать, это вполне безопасно. На самом деле, это не так. Во-первых, даже из ваших фотографий можно сделать кое-какие выводы о том, где вы живете и где учитесь. Во-вторых, такой доступ позволит незнакомцу увидеть комментарии и лайки от ваших друзей, перейти на их страницы и, если друзья более беспечны, получить информацию о вас оттуда. Например, номер школы в которой вы учитесь, что по сути то же самое, что адрес, где вас можно найти ежедневно. К тому же все мы общаемся в пабликах в социальных сетях или на каналах в Youtube, где мы не выступаем под никами в отличие от тех же игр. В результате мы делимся определенным количеством информации в рамках этого общения, а затем еще и пускаем всех незнакомых людей, с которыми случайно попали в один диалог на паблике, к себе на страницу. Это небезопасно.

Задание. Что такое двухфакторная аутентификация?

Настройки безопасности в социальной сети отвечают в первую очередь за защищенность вашего аккаунта от «угона». Обязательно настройте двухфакторную аутентификацию во всех соцсетях, где это возможно. Двухфакторная аутентификация – это дополнительная проверка любых действий, связанных с безопасностью вашего аккаунта с помощью одноразовых паролей, передаваемых на ваш номер телефона или в специальное приложение вроде Steam Guard.

Домашнее задание. Дома проверьте настройки своих аккаунтах в как минимум одной социальной сети и одном мессенджере, которыми вы пользуетесь. Напишите небольшое сочинение о том, что вы исправили в своих настройках и почему.

Даже если мы грамотно настроили приватность нашего аккаунта в социальной сети, ни в коем случае нельзя думать, что теперь мы можем писать и публиковать на своей странице все что угодно. Не забывайте, что аккаунты взламывают. И даже если мы максимально обезопасили свой, это не значит, что каждый из наших друзей, у кого есть доступ к нашим страницам, сделал то же самое. К тому же есть вещи, которые нельзя публиковать, даже если их видит только довольно ограниченный круг ваших знакомых.

Задание. Подумайте, что нельзя публиковать в социальной сети. Напишите хотя бы 5 вещей.

Во-первых, ни в коем случае нельзя публиковать личные данные, которые злоумышленники могут использовать, чтобы обмануть вас или навредить вам:

- важные документы, например, паспорт, права, карточка;
- номер телефона;
- домашний адрес;
- номер школы;
- чекины (их можно ставить только после возвращения домой, если очень хочется сообщить, что вы были в каком-то модном или интересном месте);
- данные о родственниках (их часто используют преступники в своих схемах, чтобы обмануть родителей или ребенка, используя максимум информации, которую им удалось добыть в соцсети).

Во-вторых, к данным, которые против вас могут использовать злоумышленники, относятся не только документы и факты о вашей жизни, но и рассказы о дорогих покупках или поездках. Нельзя, например, писать в соцсети о том, что вы всей семьей собираетесь отправиться в дорогостоящую поездку – это привлечет внимание воров

В-третьих, помните о том, что все, что вы размещаете в интернете, навсегда остается в интернете. Даже если вы удалили какую-то размещенную ранее информацию, вполне вероятно, что ее сохранил кто-то из ваших друзей. Это несет риски для вашей репутации как сейчас, так и в будущем. Не публикуйте и не отправляйте НИКОМУ и НИКОГДА НИЧЕГО, что вы бы не хотели, чтобы увидели ваши родители, учителя, или скажем, все ваши друзья. К этому относятся:

- Снимки и видео в обнаженном виде. НИКОГДА не соглашайтесь отправлять такие снимки и видео ни под каким предлогом. Это всегда чревато для вас серьезными неприятностями.
- Снимки и видео, где вы или кто-то из ваших друзей в неприглядном виде, нецензурно выражается, делает запрещенные вещи.
- Свое резко радикально мнение по острым политическим, религиозным и другим чувствительным вопросам: ваше мнение может измениться, а вот информация о том, что вы когда-то не лучшим образом высказались о чем-то, сохранится в сети.

KASPERSKY lab

kids.kaspersky.ru