

Урок интернет-этикета

**«ИНТЕРНЕТ ПРЕКРАСЕН,
КОГДА ОН БЕЗОПАСЕН»**

Что такое сетевой этикет?

Сетевой этикет – это набор правил для уважительного и уместного общения в Интернете.

Его часто называют этикетом интернета, однако он не является набором юридически обязательных правил, а представляет собой рекомендуемые правила этикета.

Сетевой этикет используется, в основном, для общения с незнакомыми людьми в интернете. Правила сетевого этикета в значительной степени зависят от сообщества и его участников.

Как правило, сетевой этикет определяет администратор веб-сайта или приложения для общения. В его обязанности также входит контроль соблюдения основных правил этикета и наказание за их нарушение.

Сетевой этикет: общие правила поведения.

1. Придерживайтесь в сети тех же правил поведения, которым вы следуете в реальной жизни
2. Думайте о своих собеседниках
3. Покажите себя с лучшей стороны
4. Сначала читайте, затем спрашивайте
5. Не забывайте об орфографии и пунктуации
6. Уважайте личные данные других
7. Уважайте время и возможности других
8. Прощайте другим мелкие ошибки
9. Не злоупотребляйте возможностями
10. Старайтесь избегать *словесных войн*
11. Разберитесь с правилами конкретного сообщества
12. Дискриминационные высказывания и сетевой этикет
13. Не разглашайте личную информацию
14. Используйте нейтральные псевдонимы
15. Сетевой этикет: боты и тролли
16. Правила поведения детей в интернете: не доверяйте участникам чата
17. Равенство прежде всего: никто не должен чувствовать себя чужим
18. Сетевой этикет для детей: изъясняйтесь кратко и по делу
19. Сетевой этикет и онлайн-обучение: советы для учеников
20. Доверяйте своим родителям.

Буллинг и кибербуллинг.

Буллинг — это травля, агрессивное преследование одного человека другим (другими).

Кибербуллинг — это травля в цифровом пространстве, то есть в интернете. Это могут быть оскорбления и злые шутки в сообщениях или в комментариях, публикация личной информации (например, вашего адреса, номера телефона, личных фотографий), посты с угрозами. Согласно исследованию сервиса VK, с агрессией в социальных сетях сталкивались хотя бы раз около 60% россиян.

Форм онлайн-травли достаточно много, но вот примеры основных:

- 1. Бойкот** — игнорирование жертвы в соцсетях или обрывание связи с ней. Пример: одноклассники удалили ребёнка из чата класса, он становится оторван от новостей, совместных планов, мероприятий.
- 2. Домогательство** — когда агрессор регулярно угрожает жертве в интернете, задаёт неприятные, личные вопросы или шантажирует. Пример: парень, которому отказали в знакомстве, пишет девушке на разных платформах, что знает её адрес, придёт к ней и всё равно заставит её с ним общаться.
- 3. Троллинг** — высмеивание при помощи оскорблений. Пример: подростки сделали из неудачной фотографии приятеля обидный мем.
- 4. Аутинг** — публикация личной информации без разрешения её владельца. Пример: вы поссорились с другом, и он выложил ваш номер телефона с просьбой закидать вас оскорблениями.
- 5. Диссинг** — также публикация личной информации, но той, которая может навредить репутации жертвы или разрушить её. Пример: ради мести выкладывают личные фотографии бывшей девушки.

КИБЕРБУЛЛИНГ. Читатели советуют...

- не отвечайте на оскорбления, игнорирование — самый верный способ прекратить травлю;
- добавьте обидчика в черный список в соцсети или чате;
- сообщите о серьезном случае травли администраторам социальной сети;
- постарайтесь отвлечься, поговорить с друзьями, родными;
- если родители знают, что их ребенок стал жертвой кибербуллинга, крайне важно, чтобы они объяснили ему, что он сам никоим образом в этом не виноват.



КИБЕРБУЛЛИНГ. Читатели советуют...

- не вступайте в диалог, не доказывайте свою позицию, не переходите на личности;
- нельзя оправдываться — агрессор получит необходимую реакцию и продолжит буллить;
- не воспринимайте хейтинг, как здоровую критику;
- не проживайте ситуацию в одиночку — обязательно обращайтесь за поддержкой к друзьям, близким или психологу.



Интернет и терроризм.

Большинство **террористических** организаций ведут свою деятельность, в первую очередь используя **Интернете**. Так проще захватить умы молодых людей, учитывая доступность и популярность социальных сетей в молодежной среде.

Террористические организации стремятся использовать любые коммуникационные возможности для пропаганды своих идей, привлечения новых сторонников. В Интернете существует большое количество сайтов, не связанных напрямую с террористическими организациями, но разделяющих их идеологию.

Один из **способов борьбы** с экстремистской идеологией в Интернет – это изоляция сайтов экстремистской направленности.

Наиболее действенным **способом уберечь** ребенка от влияния экстремистских и других деструктивных организаций остаются все же доверительные отношения между родителями, педагогами и детьми.

Вопрос 1. Как известно, злоумышленникам не составляет труда подобрать простой пароль от почты. Именно поэтому, Яндекс.Почта рекомендует создавать сложные пароли. Какой из этих паролей вы не считаете сложным?

- 1) qwertyasdf567 (пароль, в котором больше восьми символов)
- 2) Pripev04k@ (пароль, в котором есть большие и маленькие буквы, цифры и специальные символы)
- 3) 23051995 (дата рождения)

Вопрос 2. Что делать, если вы получили письмо от банка, в котором просят сообщить или подтвердить ваши персональные данные?

- 1) ничего не отправлять, так как банки никогда не запрашивают персональные данные - ни в письмах, ни по телефону.
- 2) отправить данные в ответном письме;
- 3) сообщить данные по телефону, указанному в письме;

Вопрос 3. Кто может стать жертвой интернет-мошенников?

- 1) любой пользователь интернета
- 2) активный пользователь социальных сетей
- 3) любитель интернет-шоппинга

Вопрос 4. Вы пытаетесь зайти на известный вам сайт, но браузер предупреждает об опасности. Ваши действия?

- 1) проигнорирую предупреждение: я уже не раз заходил на этот сайт и знаю, что он безопасен
- 2) не буду переходить на сайт: даже проверенный сайт может быть заражён

Вопрос 5. Кому можно сообщать свой платёжный пароль или код подтверждения по телефону?

- 1) сотруднику службы безопасности банка или платёжного сервиса;
- 2) никому и ни при каких обстоятельствах.
- 3) близкому человеку;

Вопрос 6. Какую информацию о банковской карточке ни в коем случае нельзя сообщать другим людям?

- 1) срок действия.
- 2) имя владельца;
- 3) пин-код и CVV;

Вопрос7. В соцсети незнакомый человек попросил вас перевести деньги на электронный кошелёк - его собаке срочно нужна дорогая операция. Как вы поступите?

- 1) прежде чем что-либо предпринять, проверите номер кошелька в интернете - возможно, на него принимают и другие переводы, например, платежи за дешёвые авиабилеты или какие-нибудь услуги;
- 2) не станете переводить деньги, но поделитесь объявлением на своей странице, чтобы смогли помочь другие;
- 3) как можно скорее сделаете пожертвование, так как операция срочная.

Вопрос8. Почему из кошелька, к которому привязана карта, платить безопаснее, чем напрямую с карты?

- 1) платёжный пароль для кошелька можно изменить в любой момент, а пин-код карты - гораздо сложнее.
- 2) в отличие от банковской карты кошелёк защищён платёжным паролем;
- 3) при оплате из кошелька не приходится указывать на сайтах данные карты, ведь она уже привязана к кошельку;

Вопрос9. Вы нашли объявление, в котором предлагается выполнить лёгкую работу за большое вознаграждение, но заплатят вам лишь после того, как вы всё сделаете. Как правильно поступить в таком случае?

- 1) не откликаться на вакансию.
- 2) связаться с работодателем и согласиться на работу при условии, что он пришлёт вам письмо, в котором гарантирует оплату;
- 3) срочно откликнуться, пока кто-нибудь вас не опередил;

Вопрос10. Как поступить, если вы получили сообщение в соцсети от друга, который просит денег взаймы?

- 1) перевести ему деньги;
- 2) переслать сообщение кому-нибудь ещё, кто сможет дать в долг;
- 3) проверить друга - спросить, например, как зовут вашего классного руководителя

Вопрос11. В каком случае стоит доверять информации, что ваш друг остался без денег на другом конце города и ему срочно нужны средства, чтобы добраться до дома?

- 1) если вам пришло смс с просьбой о помощи;
- 2) если за него позвонил другой человек и передал просьбу перевести деньги.
- 3) если он сам позвонил и рассказал об этом

Вопрос12. Где в интернете можно столкнуться с мошенничеством?

- 1) где угодно - от сообщения в соцсети до сайта известного магазина
- 2) в интернет-магазине, торгующем недорогими айфонами;
- 3) на незнакомом сайте, где предлагают работу;

Вопрос13. Ваши друзья жалуются, что с вашего аккаунта во ВКонтакте приходит спам. Ваши действия?

- 1) сменю пароль от учётной записи ВКонтакте - этого будет достаточно
- 2) попрошу друзей не переходить по ссылкам, которые приходят от меня, и напишу в техподдержку
- 3) сменю пароль от учётной записи во ВКонтакте, от почты, к которой привязан этот аккаунт, и пройду по компьютеру антивирусом

