**Этика в интернете**

|  |
| --- |
| **Сетевой этикет** (сетикет, нетикет — неологизм, является слиянием слов «сеть» http://wiki.ippk.ru/images/3/36/1218211676_butler.png(англ. net) и «этикет») — правила поведения, общения в Сети, традиции и культура интернет-сообщества, которых придерживается большинство. Это понятие появилось в середине 80-х годов XX века.    10 основных правил сетевого этикета: **Правило 1: Помните, что Вы говорите с человеком.** Одно из самых очевидных и все же самое часто нарушаемое правило в сети. Очень многие забывают, что их собеседник — не компьютер, что за буковками на экране прячется живой человек. Подействовать на него можно очень даже реально.  **Правило 2: Придерживайтесь тех же стандартов поведения, что и в реальной жизни.** Интернет создает ощущение анонимности. Кажется, что вам никто ничего не сделает, тем самым появляется заблуждение, что в сети правила поведения не так строги. Необходимо соблюдать этику общения, а также оставаться в рамках закона, как в реальном, так и в виртуальном пространстве.   **Правило 3: Помните, что вы находитесь в киберпространстве.** Если вы ведете активную сетевую жизнь — посещаете несколько сообществ и форумов, вам особенно важно помнить, какого стиля общения придерживаются местные собеседники. В большинстве давно сложившихся сетевых коллективов есть свои писаные или неписаные правила, которыми с удовольствием поделятся с новичком. Универсальным является совет — первое время посидеть в уголке, посмотреть и послушать.  **Правило 4: Уважайте время и возможности других.** Готовясь поделиться со всем миром гениальной новостью, подумайте, а всем ли именно эта новость важна. И уж если вам открытым текстом говорят «Отстань!» (или «Мне эта дискуссия совершенно не интересна»), лучше все же отстать. Так же, не следует ожидать мгновенной реакции на сообщения.  **Правило 5: Сохраняйте лицо.** Репутация в Интернете значит ничуть не меньше, чем в реальной жизни. Конечно, вся аудитория Интернета вас не узнает, но братья по интересам и сайтам могут знать вас как человека.  **Правило 6: Помогайте другим там, где можете.** В Интернете появляется только та информация, которая интересна широкому кругу людей, либо хоть немного представляет выгоду автору. Поэтому у людей могут возникнуть вопросы, ответов на которые в Сети нет. В таком случае, вся надежда лишь на добрых людей, которые могут уделить человеку 5 минут, чтобы помочь. Мир становится лучше, когда мы помогаем другим, а мы сами — счастливее.  **Правило 7: Не ввязывайтесь в конфликты.** Человека, давно живущего в Сети, как правило, узнаешь не по воспаленным красным глазам и рефлекторному подрагиванию пальцев рук, нет. Человек, давно живущий в Сети, отличается крепкими нервами. Если вы всерьез думаете, что какого-нибудь Интернетного аксакала можно удивить лихо закрученным матерным загибом, то подумайте еще немного. Желание отличиться выдает в тебе новичка куда вернее, чем ник «я-тут-новенький». К тому же, страстный спор может действительно потрепать новичку нервы.  **Правило 8: Уважайте право на частную переписку.** Не распространяйте в Сети личную информацию других людей — реальные имена, адреса, телефоны, фотографии без их согласия. Никогда.  **Правило 9: Не злоупотребляйте своими возможностями.** Виртуальное пространство предполагает различный доступ к тем или иным ресурсам, различный уровень знаний в тех или иных вопросах. Обладая преимуществами над другими пользователями, не следует направлять их против людей.  **Правило 10: Учитесь прощать другим их ошибки…** Каждый когда-то был новичком. Поэтому когда кто-то допускает ошибку - будь это опечатка в слове, неосторожный флейм, глупый вопрос или неоправданно длинный ответ - будьте к этому снисходительны. Даже если руки чешутся ответить, подумайте дважды. Если Вы обладаете хорошими манерами, это еще не значит, что Вы имеете лицензию на преподавание этих манер всем остальным. Если же Вы решили обратить внимание пользователя на его/ее ошибку, сделайте это корректно и лучше не в конференции, а в частном письме. Дайте людям возможность посомневаться. И не будьте высокомерным и надменным.  **Моветон**   * **Привлечение к себе внимания**   пример — так называемые «бампы» (bump), или «апы» (up) — сообщения для поднятия темы в форумах, где они часто сортируются по дате последней записи.   * **Флейм**   «словесная война». Это неожиданно возникшее бурное обсуждение, в процессе которого участники обычно забывают о первоначальной теме, переходят на личности и не могут остановиться.   * **Флуд**   сообщения в интернет-форумах и чатах, не несущие никакой полезной информации.   * **Спам**   сообщения, присылаемые вам от неизвестных людей или организаций, которым вы не давали на это разрешения.​   * **Оффтопик**   сетевое сообщение, выходящее за рамки заранее установленной темы общения. Например, запись на веб-форуме, не соответствующая либо общему направлению форума, либо той теме, в рамках которой запись оставлена.   * **Хотлинкинг**   включение в веб-страницу файлов-изображений или других ресурсов с чужого сервера.   * **Оверквотинг**   переполнение текста на форуме, e-mail, новостной группе избыточными цитатами.  Использование сокращений помогает заменить длинные слова или выражения и имеет несколько истоков. Раньше, когда мобильные телефоны только начали предлагать функцию текстовых сообщений (SMS), сообщения были ограничены в длину. Люди стали сокращать слова и использовать аббревиатуры просто для экономии денег. В Интернете же использование популярных аббревиатур экономит время на набор текста.  **LOL -  Laughing out loud («ржунимагу»)** «Lol», пожалуй, самое известное и широко используемое выражение Интернет-сленга. Оно часто появляется как ответ на смешную фразу или шутку. Просто добавляя «lol», можете придать высказыванию беззаботность или шутливость. Иногда бывает трудно передать сарказм, когда вы разговариваете в Интернете, и «lol» в этом случае может пригодиться. «lol» снижает серьёзность вашего послания и намекает на содержащийся в нём юмор. Некоторые люди используют lol чаще знаков препинания.  **LMFAO/LMAO (Laughing my f\*cking @ss off/ laughing my @ss off)** Похоже на «lol» в некоторой степени. Как и «lol», эта аббревиатура используется, когда кто-то говорит что-то смешное. Выражение «LMFAO» сильнее, чем «lol», и люди используют его в ответ на то, что находят особенно смешным.  **ROFL** Rolling on the floor laughing (валяюсь на полу от смеха) «ROFL» используется в тех же ситуациях, как «LMFAO» и «LMAO». Оно также породило слово «roflcopter» (ROFL + вертолет), который является еще одним способом сказать «ROFL».  **BRB (Be right back, «скоро вернусь»)** Вы можете использовать это сокращение, если вы, к примеру, должны отойти от компьютера или не сможете ответить в течение короткого периода времени.  **G2G (Got to go, «надо идти»)** Если вы хотите закончить разговор или нужно идти, чтобы сделать что-то, вы можете использовать это выражение, прежде чем уйти.  **TTYL (Talk to you later, «до связи»)** Это сокращение, как правило, используется, когда вы прощаетесь с кем-то.  http://vignette3.wikia.nocookie.net/piratesonline/images/b/b2/Cya.gif/revision/latest?cb=20110919040042**CYA (See you, «увидимся», «до скорого»)** Используется как прощание.  **IMHO/IMO (In my humble opinion/in my opinion, «на мой взгляд»)** Вы можете использовать «imo» всякий раз, когда хотите сказать «на мой взгляд» или «по моему мнению», это намного быстрее напечатать. Будьте осторожны, используя «imho», так как это может выглядеть саркастично. Сначала посмотрите в Интернете, как другие англоговорящие используют это сокращение. **HAHAHA** Интересно отметить, что смех онлайн отличается на разных языках. Тайский: 55555 Японский: WWW или 笑 Китайский: 哈哈 или 呵呵 Корейский: ㅋㅋㅋ Испанский: jajaja Греческий: хахаха  Иврит: xà xà xà или חָה-חָה-חָה |

# 15 ПРАВИЛ

## безопасного поведения в интернете

# № 1 ХРАНИТЕ ТАЙНЫ

**В информационном пространстве нам часто приходится вводить свои данные: ФИО, адрес, дату рождения, номера документов. Безопасно ли это?**

Персональные данные (имя, фамилия, адрес, дата рождения, номера документов) можно вводить только на государственных сайтах или на сайтах покупки билетов. И только в том случае, если соединение устанавливается по протоколу https. Слева от адреса сайта должен появиться значок в виде зеленого замка — это означает, что соединение защищено.

# № 2 БУДЬТЕ АНОНИМНЫ

**Создавая свой профиль в социальных сетях, нужно максимально избегать привязки к «физическому» миру.**

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать очевидный псевдоним: по нему должно быть ясно, что это не настоящее имя (ведь использовать ложные данные: «Алексей» вместо «Александр» — по правилам соцсетей запрещено).

Не надо ставить свою фотографию на аватар, если вам не исполнилось хотя бы 15-16 лет. Все дети и подростки младше этого возраста, публикуя свою фотографию, рискуют стать жертвой злоумышленника.

# № 3 НЕ РАЗГОВАРИВАЙТЕ С НЕЗНАКОМЦАМИ

**Есть несколько главных опасностей, с которыми можно столкнуться в интернете. По большому счету они мало отличаются от тех, что угрожают нам в реальной жизни. Злоумышленники здесь просто используют другие средства.**

**Буллинг.** Ребенка обзывают или травят в интернете — чаще всего без какой-либо причины, «потому что так весело». К жертве могут прицепиться из-за фотографии в профиле или из-за поста в соцсетях.  
**Педофилы.** Просят прислать личные фотографии, а при отказе угрожают расправой над членами семьи или шантажируют другими способами.  
**Мошенники.** Пытаются завладеть данными пользователя или втянуть ребенка в опасную финансовую авантюру.  
Главное средство защиты от всех этих угроз — конфиденциальность. Нельзя выкладывать свои фотографии в Cеть. Следует ограничить доступ к информации о всех сторонах своей жизни, будь то онлайн или офлайн. Сообщать их можно только проверенным людям: родным, близким и людям, которые знакомы вам лично, а не через интернет.

# № 4 РАСПОЗНАЙТЕ ЗЛОУМЫШЛЕННИКА

**На что надо обратить внимание прежде, чем вступить в диалог? Что сигнализирует об опасности?**

* Вы не знакомы с этим человеком в реальной жизни.
* Ваш собеседник явно взрослее вас.
* У него нет или очень мало друзей в соцсети.
* Собеседник о чем-то просит: сфотографироваться, прислать какие-то данные и т. д.

# № 5 ХРАНИТЕ ФОТО В НЕДОСТУПНОМ МЕСТЕ

**Правила публикации собственных фотографий очень простые —  если вы не хотите, чтобы они стали достоянием общественности, нельзя выкладывать их в интернет и отправлять кому-то с его помощью. Вообще. Даже мессенджеры «умеют» копировать переписку в «облако», так что вы можете потерять контроль над своими снимками.**

Если что-то куда-то было отправлено или где-то опубликовано, это ушло в Cеть. Важно помнить, что ни в коем случае нельзя выкладывать фотографии документов — своих или чужих. А фото других людей стоит выкладывать только в случае, если они на это согласны.

# № 6 БУДЬТЕ БДИТЕЛЬНЫ

**Плохая новость — удалить ничего не получится.**

Все, что попало в Cеть или даже в смартфон, останется там навсегда. Как правило, стереть данные из Cети невозможно. Единственный способ избежать утечки информации — не делиться ею.

# № 7 НЕ СООБЩАЙТЕ СВОЕ МЕСТОПОЛОЖЕНИЕ

**Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, проводите свободное время, в каких акциях участвуете, какие шоу и спектакли любите, как отдыхаете. Отследить местоположение человека теперь не составляет труда.**

# № 8 ВНИМАНИЕ — НА ИГРЫ

**Правила безопасности есть не только в соцсетях и мессенджерах. Все основные угрозы могут исходить и от онлайн-игр.**

Там ребенок даже более уязвим, поскольку им проще манипулировать: игровые объекты, членство в командах, внутриигровые социальные связи — все это может стать механизмом манипуляции для мошенников, педофилов или даже вербовщиков различных экстремистских группировок. Вот почему в игре нужно вести себя особенно внимательно.

# 9 УЧИТЕСЬ ЗАМЕЧАТЬ ПОДДЕЛЬНЫЕ САЙТЫ

**Фишинг — это способ выманивать у человека его данные: логин, название учетной записи и пароль.**

Происходит это так: пользователю присылают ссылку на сайт, очень похожую на настоящий адрес почтового сервиса или социальной сети. Как правило, фишеры специально покупают такие домены. Например, для mail.ru это может быть «meil.ru», а для vk.com — «vk-com.com».

Злоумышленник ждет, когда человек введет логин или пароль на поддельном сайте. Так он узнает данные, а потом использует их для входа в настоящий профиль своей жертвы.

# № 10 ТРЕНИРУЙТЕ ПАМЯТЬ

**Можно ли пользоваться сервисами, которые сохраняют пароли? Если в профиле содержится действительно важная информация, то, увы, нет. Почему?**

* Это удобно, но онлайн-сервисы для хранения паролей ненадежны.  
  Их часто взламывают и копируют оттуда пароли пользователей.
* Чаще всего жертвы узнают об этом лишь спустя какое-то время, если вообще узнают.
* Нередко такие сайты и сервисы создаются мошенниками специально для того, чтобы собирать пароли.

Пароли должны быть уникальными. Цифры и спецсимволы значительно усложняют процесс подбора. В соцсети, мессенджеры и почту безопаснее входить через приложения, а вот в браузерах ввода паролей следует избегать. Все приложения должны устанавливаться родителями или под их контролем.

# № 11 АККУРАТНЕЕ С ПОКУПКАМИ

Все сервисы, которые принимают деньги, должны иметь зеленый значок «https» рядом с названием. Если такого значка нет, лучше не пользоваться страницей. Впрочем, даже его наличие стопроцентной гарантии не дает.

Часто в пабликах «ВКонтакте» предлагают что-то купить с использованием платежной системы Qiwi. Тут тоже нужно проявлять бдительность и внимательно изучать отзывы о продавце. В соцсетях есть немало мошенников, которые после получения денег исчезают.

# № 12 ПРОВЕРЯЙТЕ ИНФОРМАЦИЮ

**Проверка информации — довольно сложный процесс, и даже взрослые люди далеко не всегда справляются с этим. Есть несколько формальных признаков того, что вы попали на «желтый» сайт, которому не стоит верить безоговорочно. Это кричащие заголовки, обилие рекламы или если читателя, который кликнул на новость, перекидывают куда-то дальше.**

# № 13 ПОЗАБОТЬТЕСЬ ОБ «ОБЛАКЕ»

**Насколько надежны хранилища, вроде «Облако» Mail.Ru, и можно ли там без опаски хранить документы?**

Специалисты говорят, что облачное хранилище можно обезопасить, если предварительно зашифровать документы с помощью PGP или использовать программу для создания архива, поместив в него отсканированные документы.

При создании архива нужно указать опцию «непрерывный архив» (solid archive) и поставить на этот архив хороший пароль.

**Например, такой:**«kn23iuhuio12njkpuiy89y7&R&TFTGIY\*(UYT&\*T^G!\*OUH\*&GYUIHJK)».  
**Или хотя бы такой:**«во#полеберезастояла123».

# № 14 СОБЛЮДАЙТЕ СЕТЕВОЙ ЭТИКЕТ