

10 ПРАВИЛ БЕЗОПАСНОГО ИНТЕРНЕТА

МАОУ СОШ №1 Г.ЯЛУТОРОВСКА

№ 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



№ 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.

Главное средство защиты от всех этих угроз — конфиденциальность.

Нельзя выкладывать свои фотографии в Сеть. 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.

Тех, кто пытается вас как-то задеть и обидеть (так называемых троллей), нужно просто игнорировать.



№ 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.

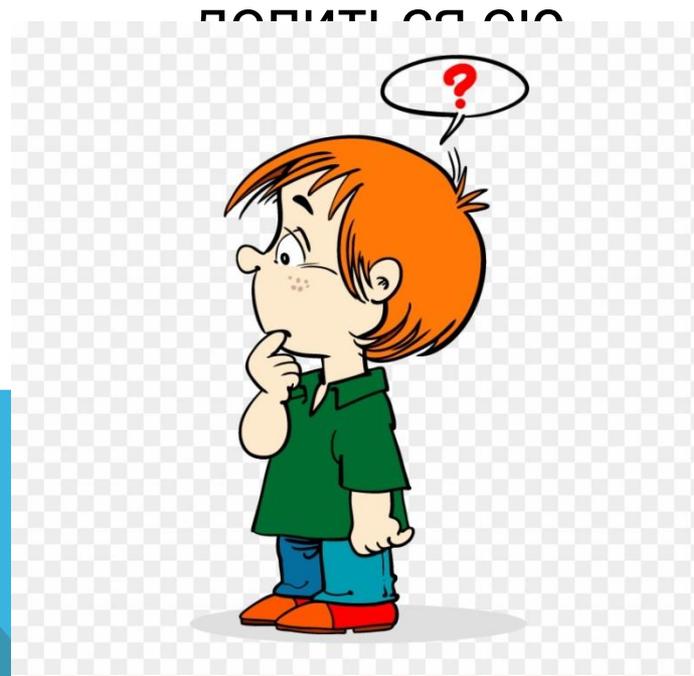
Если что-то куда-то было отправлено или где-то опубликовано, это ушло в Сеть. Важно помнить, что ни в коем случае нельзя выкладывать фотографии документов — своих или чужих. А фото других людей стоит выкладывать только если они с вами об этом согласны.



№ 6 БУДЬТЕ БДИТЕЛЬНЫ

Плохая новость — удалить ничего не получится.

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



№ 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.

Чтобы сделать геолокацию максимально безопасной, нужно следить за тем, чтобы местоположение не отображалось на «искабельных» объектах — особенно на фотографиях. На телефонах, в настройках камеры, как правило, можно запретить геометки.



№ 8 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



№ 9 СОБЛЮДАЙТЕ СЕТЕВОЙ ЭТИКЕТ

Человечество только учится общаться в Сети, но правила хорошего тона здесь ничем не отличаются от тех, которые нужно соблюдать в реальном мире. Не оскорбляйте других, не будьте навязчивым, не позволяйте своим негативным эмоциям выходить из-под контроля, пишите грамотно.

Несколько правил сетевого этикета:

- не привлекайте к себе внимание за счет эпатажа;
- не отходите от темы разговора: «флуд» считается одним из главных «грехов» в Сети;
- не игнорируйте вопросы собеседника, кроме явного троллинга или оскорблений — подобную беседу нужно немедленно прекратить;
 - никогда не участвуйте в травле: буллинг в Сети ничем не отличается от реального и одинаково опасен и для жертвы, и для



№ 10 ГЛАВНЫЙ СЕКРЕТ БЕЗОПАСНОСТИ В СЕТИ

**Не нужно делать в интернете ничего, что бы вы не стали бы делать в физическом мире.
Разница между виртуальной и реальной
действительностью минимальна.**



Спасибо за внимание!



ИСТОЧНИК:

[HTTPS://WWW.UCHEBA.RU/PROJECT/WEBSAFETY](https://www.ucheba.ru/project/websafetu)