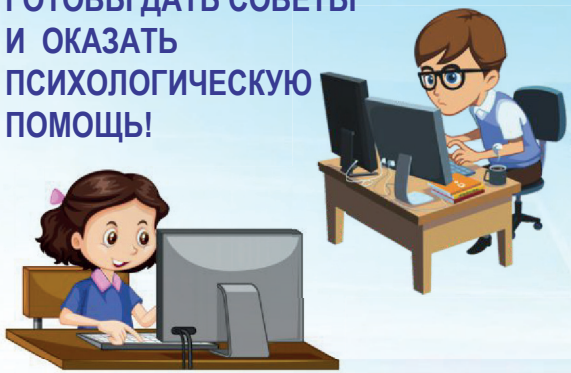
№ 8 Главный секрет безопасности в сети

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

ОБРАЩАЙСЯ В КГАУ «ЦЕНТР ПСИХОЛОГО-ПЕДАГОГИЧЕСКОЙ РЕАБИЛИТАЦИИ И КОРРЕКЦИИ», ЕСЛИ

- что-то огорчило или расстроило тебя в Интернете;
- ты стал жертвой сетевого мошенничества;
- ты столкнулся с оскорблениями и преследованиями в Интернете;
- тебе делают неприличные предложения в Интернете;
- тебе сложно поговорить с кем-то о том, что происходит с тобой в Интернете;
- родители думают, что ты слишком много времени проводишь в виртуальном мире;
- ты заметил, что тебе проще общаться с друзьями в сети, а не в реальной жизни.

СПЕЦИАЛИСТЫ НАШЕГО ЦЕНТРА ГОТОВЫ ДАТЬ СОВЕТЫ И ОКАЗАТЬ ПСИХОЛОГИЧЕСКУЮ ПОМОЩЬ!



КАМЧАТСКИЙ

ЦППРиК

КГАУ «КАМЧАТСКИЙ ЦЕНТР ПСИХОЛОГО-ПЕДАГОГИЧЕСКОЙ РЕАБИЛИТАЦИИ И КОРРЕКЦИИ»

683032, Г. ПЕТРОПАВЛОВСК-КАМЧАТСКИЙ, УЛ. ФРУНЗЕ, Д. 8
E-MAIL: CPPRKAM@MAIL.RU

ТЕЛЕФОН/ФАКС:
8 (4152) 42-05-42, 43-38-50
ОФИЦИАЛЬНЫЙ САЙТ: WWW.CPPRKAM.RU

АВТОР-СОСТАВИТЕЛЬ:
ЯНИК АЛЕНА АЛЕКСАНДРОВНА,
ПЕДАГОГ-ПСИХОЛОГ

КГАУ «КАМЧАТСКИЙ ЦЕНТР ПСИХОЛОГО-ПЕДАГОГИЧЕСКОЙ РЕАБИЛИТАЦИИ И КОРРЕКЦИИ»

БЕЗОПАСНЫЙ ИНТЕРНЕТ:

ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ

БУКЛЕТ ДЛЯ НЕСОВЕРШЕННОЛЕТНИХ

Г. ПЕТРОПАВЛОВСК-КАМЧАТСКИЙ
2021 Г.

УВАЖАЕМЫЙ ДРУГ!

Знаешь ли ты об опасностях, которые могут ждать тебя в Интернете? В этом смысле виртуальный мир не отличается от реального: там тоже есть сверстники, которые устраивают травлю, плохие компании, маньяки и мошенники. Эксперты по кибербезопасности корпорации Mail.Ru Group и портал «Учеба.ру» разработали несколько правил, следуя которым, ты сможешь оставаться в безопасности.

№ 1 Храните тайны

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

№ 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).

ГЛАВНОЕ СРЕДСТВО ЗАЩИТЫ ОТ ВСЕХ ЭТИХ УГРОЗ — КОНФИДЕНЦИАЛЬНОСТЬ!

№ 3 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-либо. Даже мессенджеры «умеют» копировать переписку в «облако», так что вы можете потерять контроль над своими снимками. 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.

№ 4 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 делиться ею.

№ 5 Не сообщайте свое местоположение

Данные геолокации позволяют всему миру узнать, где вы живете и учитесь, проводите свободное время, 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.

№ 6 Внимание — на игры

Правила безопасности есть не только в соцсетях и мессенджерах. Все основные угрозы могут исходить и от онлайн-игр. Там вы даже более уязвимы, поскольку вами 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.

№ 7 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. Существуют правила, актуальные для любых сообществ:

- **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 агрессора.**