6. 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.

7. Распознайте 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.

8. Внимание к паролям

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. Нередко такие сайты и сервисы создаются 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.

9. Соблюдайте 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.

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.

Что касается родительского поведения, то в Сети оно тоже не должно отличаться от поведения «в офлайне». От ребенка нельзя добиться повиновения путем запретов и жесткого контроля. Однако и ощущения вседозволенности в интернете тоже быть не должно. Вместе учитесь вести безопасный образ жизни, как реальной, так и виртуальной.

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №85 г. ЕКАТЕРИНБУРГ

Информационный вестник

№ 3/19-20

Безопасное поведение в Сети

Составитель: Белоцерковская О.В.

Информационные технологии всё больше проникают в общественные сферы, что вызывает значительный рост разного рода киберугроз. Чем же опасна Сеть интернет для школьников и как себя обезопасить?

Эксперты утверждают, что виртуальный мир не отличается от реального: там тоже есть сверстники, которые устраивают травлю, плохие компании, маньяки и мошенники. Маленьких детей не отпускают на улицу одних, а у подростков всегда узнают, где они, с кем, чем занимаются и когда будут дома. Такой же уровень заботы нужен и в Сети. Разница только в том, что происходящее на улице родители хорошо себе представляют, а вот ловушки, в которые можно попасть в интернете, многие пока еще не изучили до конца.

Далее приведены основные правила по безопасному поведению в интернете. Правила составлены экспертами по кибербезопасности корпорации Mail.Ru Group и порталом «Учеба.ру». Они помогут родителям, учителям и школьникам избежать различных опасностей виртуального пространства, которые окружают каждого современного ребенка и взрослого во Всемирной сети.

Правила безопасного поведения в интернете

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.

2. Будьте анонимны

Нельзя указывать свой адрес, дату рождения, школу, класс. Лучше использовать 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.

3. Не разговаривайте с незнакомцами

Есть несколько главных опасностей, с которыми можно столкнуться в интернете. 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.

Мошенники. Пытаются завладеть данными пользователя или втянуть ребенка в опасную финансовую авантюру.

Главное средство защиты от всех этих угроз — конфиденциальность. Следует ограничить доступ к информации о всех сторонах своей жизни. 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. Не сообщайте своё 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.

Для ребенка это может представлять большую опасность. Но полностью отключить геолокацию на детском телефоне нельзя. Родителям полезно использовать специальные программы, чтобы знать, где находится ребенок.

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.