В век высоких технологий информационно-телекоммуникационная сеть «Интернет» стала неотъемлемой частью жизни каждого человека. Интернет растет в глобальном масштабе. Более 4 миллиардов человек являются пользователями сети.

Информационно-телекоммуникационная сеть «Интернет» предоставляет:

1. доступ к огромному количеству полезной информации (виртуальные библиотеки, доклады, образовательный контент, новости и др.);
2. доступ к развлекательному контенту (фильмы, музыка, игры и др.)
3. возможность онлайн общения (социальные сети, мессенджеры, интернет-телефония и др.) и др.

Однако, к сожалению, в виртуальном мире очень много недобросовестных граждан (мошенники, хакеры и др.), пытающихся нанести вред пользователям сети. Обезопасить себя не так уж и трудно – достаточно соблюдать простые правила.

Данный раздел интернет-ресурса Центра цифровизации образования Республиканской естественно-математической разработан с целью повышения уровня информированности родителей и их детей о рисках и угрозах, существующих в информационно-телекоммуникационной сети «Интернет», а также методам защиты от них.

ДЛЯ ДЕТЕЙ

Следует придерживаться 4 простых правил:

Правило №1

Всегда используйте сложный пароль, содержащий заглавные и строчные буквы (A, B, C, D…), цифры (0,1…9) и специальные символы (!,\*,?…). Следует создавать индивидуальные(новые) пароли для каждой учетной записи. Статистика показывает, что чаще всего пользователи используют пароль «123456» или дату своего рождения. Взлом такого пароля не составит труда для злоумышленника. Запомните: пароль – ключ от сейфа, который должен быть надежным и секретным, никто не должен знать его кроме Вас.

**Пример надежного пароля: dTwI2583!**

Правило №2

Устройству, которое Вы используете для выхода в сеть «Интернет» может навредить вредоносное программное обеспечение (вирусы), которого с каждым днем становится все больше на просторах сети «Интернет». Вирусы могут скопировать, уничтожить, изменить информацию на Вашем устройства, использовать его для атаки на другие устройства, отследить Ваши действия.

Для защиты устройства используйте лицензионное антивирусное программное обеспечение с актуальными обновлениями. Регулярно обновляйте его. Старайтесь не посещать подозрительные сайты (файлообменники, торренты и др.).

Следуйте рекомендациям Вашего лицензионного антивирусного программного обеспечения.

Правило №3



В сети «Интернет» есть не только злоумышленники, но и просто невоспитанные люди, пытающиеся для собственного развлечения разместить провокационные сообщения, чтобы вызвать конфликт. Не реагируйте на такого рода сообщения, прекрати диалог с данным человеком и сообщите родителям о случившемся.

Правило №4



Никогда и никому не сообщайте свои персональные данные в сети «Интернет». Номер телефона, адрес дома, паспортные данные, школа, в которой Вы учитесь – вся эта информация может быть использована злоумышленником, чтобы навредить Вам. Если при регистрации на интернет-ресурсе Вас просят предоставить данную информацию, посоветуйтесь с родителями.

ДЛЯ РОДИТЕЛЕЙ

**4 основных совета:**

Совет №1



Расскажите ребенку об опасностях, с которыми он может столкнуться в сети «Интернет» – вредоносные программы, мошенники, интернет-травля и др. Покажите ему видеоуроки, позволяющие наглядно продемонстрировать возможные ситуации и правильное поведение в них.

Совет №2



Используйте всевозможные инструменты для организации родительского контроля. Сегодня почти всё лицензионные антивирусное программное обеспечение содержит модуль родительского контроля, позволяющий защитить ребенка от нежелательного контента и вредоносного программного обеспечения. Регулярного обновляйте антивирусное программное обеспечение на всех устройствах, имеющих доступ к сети «Интернет».

Совет №3



Проведите разъяснительную работу с ребенком на тему важности использования надежного пароля. Объясните ему, что чем сложнее его пароль, тем безопаснее информация, которую защищает этот пароль.  На личном примере продемонстрируйте как правильно создать безопасный пароль.

Совет №4



Контролируйте ребенка при работе в сети «Интернет». Детей дошкольного и младшего школьного возраста не следует оставлять «один на один» с глобальной сетью. Обучайте его методам работы в сети «Интернет», знакомьте с официальными надёжными сайтами. Расскажите ему о том, что не следует размещать личную (персональную) информацию о себе в сети «Интернет».