Родителям «Информационная безопасность детей»

Вирусы скрытно проникают в компьютерные системы, и без эффективной защиты бороться с ними невозможно. Чтобы вирусы проникли в компьютер, достаточно всего лишь открыть вложение в электронном письме (при этом совершенно не обязательно, чтобы письмо было отправлено неизвестным адресатом, хорошо известный компаньон также может прислать вирус, если ранее его компьютер был заражён). Некоторым вирусам достаточно уже того, что компьютер просто подключён к локальной сети, к которой подключён и заражённый компьютер.

Спам не только вызывает раздражение у пользователей, но и забивает каналы связи, расходует трафик, отвлекает от работы, вынуждая людей искать важную корреспонденцию среди рекламы. В конечном счёте всё это приводит к финансовым потерям. Помимо этого, спам также является одним из распространённых каналов внедрения троянских программ и вирусов.

Фишинг, в отличие от спама, нацелен на узкие группы пользователей и содержит сообщения с социальным контекстом, призывающие потенциальную жертву открыть исполняемый файл или перейти на сайт, содержащий вредоносный код.

Большую опасность представляет также **удалённый взлом компьютеров**, за счёт которого злоумышленники могут получать возможность читать и редактировать документы, хранящиеся на файл-серверах и в компьютерах, по собственному желанию уничтожать их, внедрять собственные программы, которые следят за всеми действиями конкурентов и собирают определённую информацию, вплоть до незаметного аудио- и видеонаблюдения через микрофоны ноутбуков и штатные веб-камеры.

Одной из самых распространённых угроз, связанных с общением в Сети, является кибербуллинг.

Это форма запугивания, насилия и травли детей с помощью телефонов и Интернета. Кибербуллинг опасен не меньше, чем издевательства в привычном понимании, ведь жертва кибербуллинга находится в большом психологическом напряжении, и не каждый ребёнок сможет его вынести самостоятельно.

Совет 1. Далеко не всему и не всем в Сети можно доверять. Нельзя публиковать онлайн домашний адрес, слишком много рассказывать о себе и своей семье, хвастаться дорогими гаджетами и игрушками.

Совет 2. Помните, что за всё сказанное и сделанное в Интернете придётся отвечать. Все действия можно отследить, поэтому не стоит совершать необдуманных поступков.

Совет 3. Нельзя скачивать файлы с подозрительных сайтов, из писем и сообщений неизвестных отправителей. Использьзуйте настройки конфиденциальности и закройте профили в социальных сетях, пусть они будут только для друзей. Не надо добавлять в друзей всех подряд. Лучше всего, если это будут лично знакомые или хотя бы друзья друзей.

Совет 4. Не реагируйте на киберагрессию. Хамство и троллинг в Интернете - признак скверного воспитания и неуверенности в себе. Если кто-то будет писать вам оскорбительные сообщения или угрожать, расскажите об этом родителям, а вот оппонента следует игнорировать. Отсутствие ответа будет лучшим наказанием для интернет-агрессора, и он скоро потеряет интерес. Самый лучший способ — просто заблокировать обидчика (внести его в чёрный список) самостоятельно или с помощью модератора — пользователя форума или сайта, который следит за соблюдением правил ресурса, имеет право редактировать и удалять сообщения других пользователей и вносить их в чёрный список (банить).

Совет 5. Ни в коем случае нельзя общаться с посторонними взрослыми людьми, особенно если они просят прислать фотографии или предлагают встретиться. Сразу же сообщите родителям, если такое произойдёт.