ПРОФИЛАКТИКА

И БОРЬБА С ОСНОВНЫМИ РИСКАМИ ИНТЕРНЕТА

ДЛЯ РОДИТЕЛЕЙ И УЧИТЕЛЕЙ

ВРЕДОНОСНОЕ ПО

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред и нарушить конфиденциальность хранящейся в нем информации.

Подобные программы чаще всего снижают скорость обмена данными с Интернетом, а также могут использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флешки и т.д.), но и через электронную почту посредством спама или скачанных из Интернета файлов.

Установите на компьютеры антивирусные программы и почтовые фильтры для предотвращения заражения компьютера и потери ваших данных. Подобные программы наблюдают за трафиком и могут остановить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно компьютерные игры.

ПРОФИЛАКТИКА

И БОРЬБА С ОСНОВНЫМИ РИСКАМИ ИНТЕРНЕТА

ВРЕДОНОСНОЕ ПО

ДЛЯ РОДИТЕЛЕЙ И УЧИТЕЛЕЙ

- Никогда не открывайте вложения, присланные с подозрительных и неизвестных вам адресов.
- Следите за тем, чтобы ваш антивирус регулярно обновлялся, и раз в неделю проверяйте компьютер на вирусы.
- Регулярно делайте резервную копию важных данных, а также научите это делать ваших детей.
- Старайтесь периодически менять пароли, но не используйте слишком простые пароли, которые можно легко взломать (даты рождения, номера телефонов и т. п).
- Расскажите ребенку, что нельзя рассказывать никакие пароли своим друзьям и знакомым. Если пароль стал кому-либо известен, то его необходимо срочно поменять.
- Расскажите ребенку, что, если он пользуется Интернетом с помощью чужого устройства, он должен не забывать выходить из своего аккаунта в социальной сети, в почте и на других сайтах после завершения работы.
- Никогда не следует сохранять на чужом компьютере свои пароли, личные файлы, историю переписки — по этой информации злоумышленники могут многое узнать о вашем ребенке.

ПРОФИЛАКТИКА

И БОРЬБА С ОСНОВНЫМИ РИСКАМИ ИНТЕРНЕТА

ДЛЯ РОДИТЕЛЕЙ И УЧИТЕЛЕЙ

КИБЕРМОШЕННИЧЕСТВО

Кибермошенничество — один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.).

Отправка любых смс на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Проинформируйте ребенка о самых распространенных методах мошенничества в сети. Всегда совместно принимайте решение о том, стоит ли воспользоваться теми или иными услугами, предлагаемыми в Интернете.

Не оставляйте в свободном для ребенка доступе банковские карты и платежные данные, воспользовавшись которыми ребенок может самостоятельно совершать покупки.

Не отправляйте о себе слишком много информации при совершении интернет-покупок. Помните, что никогда модератор сайта не потребует полные данные вашего счета, пароли и пин-коды. Если кто-то запрашивает подобные данные, будьте бдительны – скорее всего, это мошенники.

Установите на свои компьютеры антивирус или персональный брандмауэр. Подобные приложения наблюдают за трафиком и могут предотвратить кражу конфиденциальных данных или другие подобные действия.

ПРОФИЛАКТИКА

И БОРЬБА С ОСНОВНЫМИ РИСКАМИ ИНТЕРНЕТА

ДЛЯ РОДИТЕЛЕЙ И УЧИТЕЛЕЙ

КИБЕРБУЛЛИНГ

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных Интернет-сервисов.

Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не стоит писать резкие и оскорбительные слова – читать грубости так же неприятно, как и слышать.

Научите детей правильно реагировать на обидные слова или действия других пользователей. Не стоит общаться с агрессором, и тем более пытаться ответить ему тем же. Возможно стоит вообще покинуть данный ресурс и удалить оттуда свою личную информацию, если не получается решить проблему мирным путем.

Если у вас есть информация, что кто-то из друзей или знакомых вашего ребенка подвергается кибербуллингу, то сообщите об этом классному руководителю или школьному психологу – необходимо принять меры по защите ребенка.

Объясните детям, что личная информация, которую они выкладывают в Интернете (домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, личные фотографии) может быть использована агрессорами против них.

Помогите ребенку найти выход из ситуации – практически на всех форумах и сайтах есть возможность заблокировать обидчика, написать жалобу модератору или администрации сайта, потребовать удаление странички.

ПРОФИЛАКТИКА

И БОРЬБА С ОСНОВНЫМИ РИСКАМИ ИНТЕРНЕТА

ДЛЯ РОДИТЕЛЕЙ И УЧИТЕЛЕЙ

ИНТЕРНЕТ-ЗАВИСИМОСТЬ

Интернет-зависимость — навязчивое желание войти в Интернет, находясь офлайн и неспособность выйти из Интернета, будучи онлайн. Исследователи отмечают, что большая часть Интернет-зависимых (91%) пользуется сервисами Интернета, связанными с общением. Другую часть зависимых (9%) привлекают сервисы сети информационного характера.

Оцените, сколько времени ваш ребенок проводит в сети, не пренебрегает ли он из-за работы за компьютером своими домашними обязанностями, выполнением уроков, сном, полноценным питанием, прогулками.

Поговорите с ребенком о том, чем он занимается в Интернете. Социальные сети создают иллюзию полной занятости — чем больше ребенок общается, тем больше у него друзей, тем больший объем информации ему нужно охватить — ответить на все сообщения, проследить за всеми событиями, показать себя.

Выясните, поддерживается ли интерес вашего ребенка реальными увлечениями, или же он просто старается ничего не пропустить и следит за обновлениями ради самого процесса. Постарайтесь узнать, насколько важно для ребенка общение в сети и не заменяет ли оно реальное общение с друзьями.

Понаблюдайте за сменой настроения и поведения вашего ребенка после выхода из Интернета. Возможно проявление таких психических симптомов как подавленность, раздражительность, беспокойство, нежелание общаться.

ПРОФИЛАКТИКА

И БОРЬБА С ОСНОВНЫМИ РИСКАМИ ИНТЕРНЕТА

ДЛЯ РОДИТЕЛЕЙ И УЧИТЕЛЕЙ

КАК СПРАВЛЯТЬСЯ С ИНТЕРНЕТ-ЗАВИСИМОСТЬЮ

- Постарайтесь наладить контакт с ребенком. Узнайте, что ему интересно, что его беспокоит и т.д.
- Не запрещайте ребенку пользоваться Интернетом, но постарайтесь установить регламент пользования. Для этого можно использовать специальные программы родительского контроля, ограничивающие время в сети.
- Ограничьте возможность доступа к Интернету только своим компьютером или компьютером, находящимся в общей комнате — это позволит легче контролировать деятельность ребенка в сети. Следите за тем, какие сайты посещает Ваш ребенок.
- Попросите ребенка подробно записывать, на что тратится время, проводимое в Интернете. Это поможет наглядно увидеть проблему, а также избавиться от некоторых навязчивых действий — например, от бездумного обновления странички в ожидании новых сообщений.
- Предложите своему ребенку заняться чем-то вместе, постарайтесь его чем-то увлечь. Попробуйте перенести кибердеятельность в реальную жизнь. Важно, чтобы у ребенка были не связанные с Интернетом увлечения, которым он мог бы посвящать свое свободное время.
- Дети с Интернет-зависимостью субъективно ощущают невозможность обходиться без сети. Важно, чтобы ребенок понял — ничего не произойдет, если он на некоторое время «выпадет» из жизни Интернет-сообщества.