ПАМЯТКА ДЛЯ ДЕТЕЙ ПО БЕЗОПАСНОМУ ПОВЕДЕНИЮ В ИНТЕРНЕТЕ

Для того чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, ребенок должен предпринимать следующие меры предосторожности при работе в Интернете:

- Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
- Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.
- Если вас что-то пугает в работе компьютера, немедленно выключите его. Расскажите об этом родителям или другим взрослым.
- Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
- Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
- Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете. О подобных предложениях немедленно расскажите родителям.
- Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки. Расскажите об этом родителям.

–

<u>При подключении к Интернету выполняйте следующие основные правила для обеспечения защиты устройств, информации и членов семьи</u>

Защитите свой компьютер

• Постоянно обновляйте все программное обеспечение (включая веб-браузер),
• Установите законное антивирусное и антишпионское программное обеспечение.
• Брандмауэр должен быть всегда включен. Брандмауэр – это программный или аппаратный комплекс, который проверяет данные, входящие через Интернет или сеть, и, в зависимости от настроек брандмауэра, блокирует их или позволяет им пройти в компьютер.
• Установите защиту с помощью пароля.
• Не вставляйте неизвестные флеш-накопители (или USB-накопители) в свой компьютер. Если на них имеется вирус, этот вирус может заразить ваш компьютер.

Используйте надежные пароли и храните их в секрете

• Придумайте пароли, представляющие собой длинные фразы или предложения и содержащие сочетание строчных, прописных букв, цифр и символов. Не храните пароль в браузере или на каком-либо сайте. Нельзя использовать одинаковые пароли для разных сайтов и нескольких аккаунтов (информация, при помощи которой любая система распознает Вас, проще говоря, авторизует для доступа), особенно для аккаунтов электронной почты.

Обеспечьте защиту секретной личной информации

• Прежде чем вводить секретные сведения в веб-форме или на веб-странице, обратите внимание на наличие таких признаков, как адрес веб-страницы, начинающийся с префикса https и значка в виде закрытого замка ( ) рядом с адресной строкой, который обозначает безопасное соединение.

Основы безопасного поведения в сети Интернет

1. Посещайте веб-страницы с осторожностью. Не открывайте всплывающие окошки и яркую рекламу — это могут быть скрытые ссылки на вирусные программы. Не отвлекайтесь на баннеры с предложениями сыграть в игру или получить выигрыш. Мошеннические способы привлечения посетителей на порнографические или фальшивые сайты становятся все более изобретательными. Можно дополнительно установить специальную программу для браузера, которая будет отключать большинство всплывающих окон.
2. Прежде чем открывать вложение или переходить по ссылке, приведенной в сообщении электронной почты, мгновенном сообщении или в социальной сети, убедитесь, что отправитель действительно отправлял сообщение. Не переходите по ссылкам и не нажимайте кнопки во всплывающих сообщениях, которые кажутся подозрительными.
3. Никогда не предоставляйте секретные сведения (такие как номер счета или пароль) в ответе на сообщение электронной почты, мгновенное сообщение или социальной сети.
4. Никогда не отвечайте на просьбы прислать деньги от «членов семьи», на предложения о сделке, которые слишком хороши, чтобы быть правдой, на

сообщения о розыгрышах лотереи, в которых вы не участвовали, или другие мошеннические сообщения.

5. Безопасно используйте социальные сети. Откройте *пункт «Настройки» или «Параметры»* в таких службах, как Facebook и Twitter, чтобы настроить список пользователей, которые могут просматривать ваш профиль или фотографии, помеченные вашим именем, контролировать способы поиска информации и добавления комментариев о вас, а также узнать, как можно заблокировать некоторых пользователей. Никогда не публикуйте информацию, которую вы не хотели бы видеть на доске объявлений.

Подходите избирательно к предложениям дружбы. Периодически анализируйте, кто имеет доступ к вашим страницам, а также просматривайте информацию, которую эти пользователи публикуют о вас.

Советы учителю, организующему обучение с помощью Интернет-ресурсов, по обеспечению безопасности:

- приучайте детей не «проводить время» в Интернете, а активно пользоваться полезными возможностями сети (презентации; слайд-шоу и т.п.);
- поощряйте обучающихся использовать различные источники, такие как библиотеки;
- используйте закрытые среды обучения, например, учебные блоги, где могут оставлять свои комментарии только те, кто получил соответствующий доступ от учителя, ведущего блог;
-научите ребенка пользоваться поиском в Интернет. Покажите, как использовать различные поисковые машины для осуществления поиска;
- формулируйте конкретную учебную задачу: что хочу найти? где? как использую?
- опирайтесь на список проверенных учителем ресурсов, с которых предлагается использовать информацию;

Полезные сайты:

Сайт «Защита детей от вредной информации в Интернет» - www.internet-kontrol.ru/stati/bezopasnost-detey-v-internete.html;

Сайт «Личная безопасность» - www.obzh.info;

Сообщество «Начальная школа» - http://www.nachalka.com/bezopasnost

Советы по обеспечению родительского контроля в Интернете с помощью Родительского контроля в Windows Vista, средств Родительского контроля, встроенных в Kaspersky Internet Security - http://www.oszone.net/6213/