БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ. ИНФОРМАЦИОННАЯ ПАМЯТКА

- **Контакты с незнакомыми людьми с помощью чатов или электронной почты.** Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.
- **Неконтролируемые покупки.** Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

- **Угроза заражения вредоносным ПО.**

  Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов.

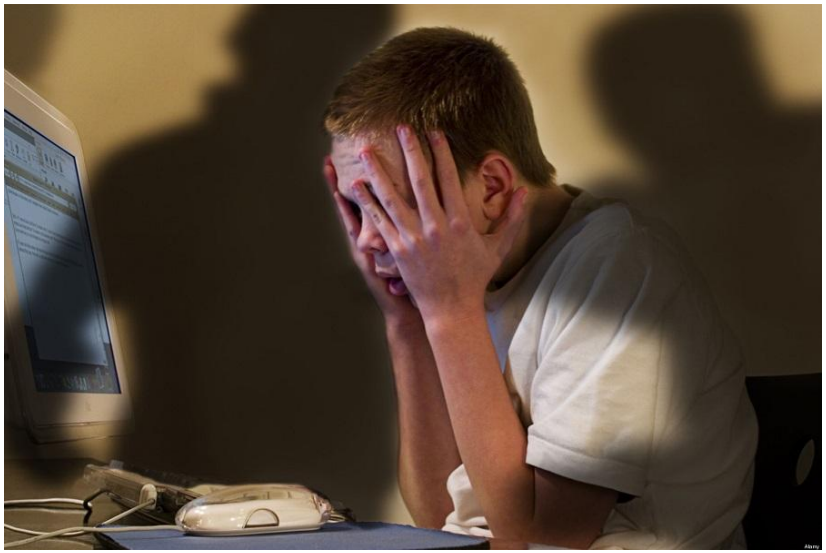
Доступ к неподходящей информации:

- сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности;
- сайты, размещающие изображения порнографического или иного неприемлемого сексуального контента, к которым дети могут легко получить доступ;
- сайты с рекламой табака и алкоголя;
- сайты, посвященные изготовлению взрывчатых веществ;
- сайты, пропагандирующие наркотики;
- сайты, пропагандирующие насилие и нетерпимость;
- сайты, публикующие дезинформацию;
- сайты, где продают оружие, наркотики, отравляющие вещества, алкоголь;
- сайты, позволяющие детям принимать участие в азартных играх онлайн;
- сайты, на которых могут собирать и продавать частную информацию о Ваших детях и Вашей семье.

- Ребенку не следует давать частной информации о себе (фамилию, номер телефона, адрес, номер школы) без разрешения родителей.
- Ребенку нужно знать, что нельзя через Интернет давать сведения о своем имени, возрасте, номере телефона, номере школы или домашнем адресе, и т.д. Убедитесь, что у него нет доступа к номеру кредитной карты или банковским данным. Научите ребенка использовать прозвища (ники) при общении через Интернет: анонимность - отличный способ защиты. Не выкладывайте фотографии ребенка на веб-страницах или публичных форумах.

- Не следует открывать письма электронной почты, файлы или Web-страницы, полученные от людей, которые не знакомы или не внушают доверия.
- Научите его, как следует поступать при столкновении с подозрительным материалом, расскажите, что не нужно нажимать на ссылки в электронных сообщениях от неизвестных источников, открывать различные вложения. Такие ссылки могут вести на нежелательные сайты, или содержать вирусы, которые заразят Ваш компьютер. Удаляйте с Вашего компьютера следы информации, которую нежелательно обнаружить Вашему ребенку.

- Встреча в реальной жизни со знакомыми по Интернет-общению не является очень хорошей идеей, поскольку люди могут быть разными в электронном общении и при реальной встрече, и, если ребенок желает встретиться с ними, родителям следует пойти на первую встречу вместе.
- Отсутствием возможности видеть и слышать других пользователей легко воспользоваться. И 10-летний друг Вашего ребенка по чату в реальности может оказаться злоумышленником. Поэтому запретите ребенку назначать встречи с виртуальными знакомыми



- Установите несколько четких и жестких правил для ребенка, чтобы контролировать расписание, время подключения и способ использования им Интернета. Убедитесь, что установленные правила выполняются. Особенно важно контролировать выход ребенка в Интернет в ночное время.
- Хороший антивирус – союзник в защите Вашего ребенка от опасностей Интернета.
- Ребенку не следует давать свой пароль кому-либо, за исключением взрослых членов семьи.
- Следует объяснить ребенку, что он не должен делать того, что может стоить семье денег, кроме случаев, когда рядом с ним находятся родители.

ИНСТРУКЦИЯ ПО БЕЗОПАСНОМУ ОБЩЕНИЮ В ЧАТЕ

1. Не доверяйте никому вашу личную информацию.
2. Сообщайте администратору чата о проявлениях оскорбительного поведения участников.
3. Если вам неприятно находиться в чате, покиньте его.
4. Если вам что-то не понравилось, обязательно расскажите об этом родителям.
5. Будьте тактичны по отношению к другим людям в чате.

ИНТЕРНЕТ ЭТИКА

- Узнайте правила прежде, чем что-нибудь сказать или сделать.
- Думайте прежде, чем что-либо напечатать. Удостоверьтесь, что Вы говорите приемлемые вещи, которые не приведут к разгоревшемуся конфликту. Единственное, в чем Вы можете не сомневаться – это в том, что все, сказанное Вами в Интернете, может вернуться и неотступно преследовать Вас.
- Не относитесь критически к другим, особенно к новичкам, даже если они нарушают правила. Если Вы должны помочь кому-то или исправить кого-то, сделайте это по электронной почте, а не на общественном форуме (например, в чате). Помните, что и Вы когда-то были новичком.
- Не тратьте время других пользователей впустую. Не посылайте цепочку электронных писем, не передавайте киберслухи, не разыгрывайте других, не рассылайте спам.
- Защищайте личную жизнь и личную информацию других пользователей. Не публикуйте в онлайне чей-либо адрес электронной почты без разрешения владельца. Вместо этого можно использоваться опцию «Отправить по электронной почте». Не используйте без разрешения чужой пароль.
- Не присваивайте вещи, не платя за них (в основном это касается условно-бесплатного программного обеспечения).

ПРАВИЛА БЕЗОПАСНОСТИ ДЛЯ ОБЩЕДОСТУПНОГО КОМПЬЮТЕРА

1. *Не сохраняйте свои учетные данные для входа в систему.*
2. *Не оставляйте без присмотра компьютер с важными сведениями на экране.*
3. *Заметайте свои следы.*
4. *Опасайтесь подглядывания через плечо.*
5. *Не вводите важные сведения на общедоступном компьютере.*