



## Информационная безопасность

Памятка для обучающихся об информационной безопасности

### **НЕЛЬЗЯ**

1. Всем подряд сообщать свою частную информацию настоящие имя, фамилию, телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей;
2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;
3. Грубить, придирается, оказывать давление — вести себя невежливо и агрессивно;
4. Не распоряжайся деньгами твоей семьи без разрешения старших - всегда спрашивай родителей;
5. Не встречайся с Интернет - знакомыми в реальной жизни - посоветуйся со взрослым, которому доверяешь.

### **ОСТОРОЖНО**

1. Не все пишут правду. Читаешь о себе неправду в Интернете — сообщи об этом своим родителям или опекунам;
2. Приглашают переписываться, играть, обмениваться - проверь, нет ли подвоха;
3. Незаконное копирование файлов в Интернете - воровство;
4. Всегда рассказывай взрослым о проблемах в сети - они всегда помогут;
5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунты в соцсетях и других порталах.

### **МОЖНО**

1. Уважай других пользователей;
2. Пользуешься Интернет- источником - делай ссылку на него;
3. Открывай только те ссылки, в которых уверен;
4. Общаться за помощью к взрослым - родители, опекуны и администрация сайтов они всегда помогут;
5. Пройди обучение на сайте «Сетевичок» и получи паспорт цифрового гражданина!

## Советы родителям по обеспечению безопасности ребенка в Интернете

### *Какие угрозы содержит Интернет?*

1. «Угроза заражения вредоносным программным обеспечением (ПО)». Ведь 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 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.
2. «Доступ к нежелательному содержимому». Ведь сегодня дела обстоят таким образом, что любой ребенок, выходящий в Интернет, может просматривать любые материалы. А это насилие, наркотики, порнография, страницы, подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи), убийствам, страницы с националистической или откровенно фашистской идеологией и многое-многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера.
3. «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;
4. «Неконтролируемые покупки». Эта угроза в настоящее время стала весьма актуальной.

### **Рекомендации, которые, возможно, помогут Вам защитить своего ребенка:**

- 1) Посещайте Интернет вместе с детьми. Поощряйте ваших детей делиться с вами их успехами и неудачами в деле освоения Интернет.
- 2) Объясните детям, что если в Интернет что-либо беспокоит их, то им следует не скрывать этого, а поделиться с вами своим беспокойством.
- 3) Объясните ребенку, что при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т. д.), использовании он-лайн игр и других ситуациях, требующих регистрации,

нельзя использовать реальное имя, помогите вашему ребенку выбрать регистрационное имя, не содержащее никакой личной информации.

4) Объясните ребенку, что нельзя выдавать свои личные данные, такие как домашний адрес, номер телефона и любую другую личную информацию, например, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т. д.

5) Объясните своему ребенку, что в реальной жизни и в Интернет нет разницы между неправильными и правильными поступками.

6) Научите ваших детей уважать собеседников в Интернет. Убедитесь, что они понимают, что правила хорошего тона действуют одинаково в Интернет и в реальной жизни.

7) Скажите им, что не стоит встречаться с друзьями из Интернет. Ведь люди могут оказаться совсем не теми, за кого себя выдают.

8) Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернет – правда. Приучите их спрашивать о том, в чем они не уверены.

9) Не забывайте контролировать детей в Интернет с помощью специального программного обеспечения. Это поможет вам отфильтровывать вредоносное содержание, выяснить, какие сайты на самом деле посещает ваш ребенок и что он там делает.

10) Регулярно проверяйте список контактов своих детей, чтобы убедиться, что они знают всех, с кем они общаются.

11) Внимательно проверяйте запросы на включение в список новых друзей. Помните, что в Интернете человек может оказаться не тем, за кого он себя выдает.

12) Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернет.

13) Периодически, а лучше ежедневно проверяйте отчеты, на какие сайты заходил Ваш ребенок. Это можно сделать через Родительский контроль (см. далее) или то, что вы сможете увидеть во временных файлах Интернет (папки c:\Users\User\AppData\Local\Microsoft\Windows\Temporary Internet Files в операционной системе Windows Vista).

14) Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.

15) Покажите ребенку, что вы наблюдаете за ним не только потому что вам это хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.

16) Детям до 10 лет рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку.