**Как научить ребенка быть осторожным в Сети и не стать жертвой**

**интернет-мошенников**  
 Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб.

Предупреждение кибермошенничества:

* Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете.
* Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.
* Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности, ознакомьтесь с отзывами покупателей:

1. проверьте реквизиты и название юридического лица – владельца магазина;
2. уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs) ;
3. поинтересуйтесь, выдает ли магазин кассовый чек;
4. сравните цены в разных интернет-магазинах;
5. позвоните в справочную магазина;
6. обратите внимание на правила интернет-магазина;
7. выясните, сколько точно вам придется заплатить.

**Как научить ребенка не загружать на компьютер вредоносные программы**

Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать Ваш компьютер для распространения вируса, рассылать от Вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Предупреждение столкновения с вредоносными программами:

* Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить 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 игр. Объясните ребенку, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
* Периодически старайтесь полностью проверять свои домашние компьютеры. Делайте резервную копию важных данных. Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

**Как защититься от СПАМА**

  Стопроцентно защититься от СПАМа невозможно. Но можно свести к минимуму вероятность его попадания в вашу деловую или личную почту следующими простыми мерами:

* Не сообщайте свой электронный адрес никому, кроме людей, которым доверяете.
* Не указывайте ваш e-mail в формах опросов и гостевых книгах.
* При работе с интернет-магазинами и прочими сервисами используйте отдельный   
  e-mail, который вы не используете для важных дел.
* Ни в коем случае не публикуйте свой электронный адрес в открытом доступе. В icq, на форумах, сайтах знакомств и вообще везде, где его могут увидеть посторонние.
* При выборе названия почтового ящика не используйте простые названия, которые спамеры могут подобрать «в уме».
* При работе в icq скрывайте информацию о себе. Запретите писать неавторизованным пользователям и пользуйтесь анти-спам защитой.
* В социальных сетях установите настройки приватности на максимальный уровень. Если это возможно, запретите всем, кроме друзей, писать в социальной сети. То же самое касается личных сообщений.
* Держите включенными все возможные анти-спам системы. Таковые имеются в почтовых клиентах, службах мгновенной доставки сообщений, антивирусах (например, Kaspersky Anti-Spam) и фаерволах.
* Запретите всплывающие окна в своем браузере, это спасет вас от переходов на ненужные страницы.

В интернете существует множество сайтов, борющихся со спамом. Например, проект «Антиспам.РУ» (antispam.ru). Также в Сети можно найти немало фильтров для контроля действий спамеров, как платных, так и бесплатных (например, spamfi ghter.com). Настройка фильтра приема почты позволяет распознать нежелательные письма и заранее поместить в корзину или специально отведенную папку. Бесплатным фильтром является «черный список» на большинстве почтовых серверов, который запоминает адреса, с которых приходит спам и блокирует их. Минусом сервиса является то, что в «черный список» попадают почтовые ящики обычных пользователей, что приводит к потере писем. Фильтр по теме письма работает эффективнее, но и его многие спамеры научились обходить.