**Защитите свой компьютер**

* + Постоянно обновляйте все программное обеспечение (включая веб-браузер), используя [Центр обновления Microsoft](http://go.microsoft.com/fwlink/p/?LinkId=148275).
  + Установите законное антивирусное и антишпионское программное обеспечение, такое как [Microsoft Security Essentials](http://go.microsoft.com/fwlink/p/?LinkId=168949).
  + Брандмауэр должен быть всегда включен.
  + Установите на беспроводном маршрутизаторе 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.
  + 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.

**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 http**s** и значка в виде закрытого замка () рядом с адресной строкой, который обозначает безопасное соединение.
  + Никогда не предоставляйте секретные сведения (такие как номер счета или пароль) в ответе на сообщение электронной почты, мгновенное сообщение или социальной сети.
  + 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.

**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. Используйте на разных сайтах разные пароли, особенно на тех, где хранится финансовая информация.

**Позаботьтесь о своей безопасности и репутации в Интернете**

* + 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.

**Поговорите с детьми о безопасности в Интернете**

Чтобы предпринять комплексные меры по обеспечению безопасности в Интернете, инструктируйте своих детей и контролируйте их действия в Интернете. Договоритесь о четких правилах просмотра веб-страниц и игр в Интернете, опираясь на зрелость ваших детей и семейные ценности. Обращайте внимание на то, чем занимаются ваши дети в Интернете и с кем они там общаются