

«Безопасность детей в Интернет»

Правовые, психологические, технические аспекты безопасной работы в Интернет

Интернет — мир широких возможностей



Интернет позволяет вам:

- общаться с друзьями, семьей, коллегами;
- получать доступ к информации и развлечениям;
- учиться, встречаться с людьми и узнавать новое.

Защита и безопасность в Интернете

Защита. Необходимо защищать компьютеры при помощи современных технологий подобно тому, как мы защищаем двери в наших домах.

Безопасность. Наше поведение должно защищать от опасностей Интернета.



Основные угрозы безопасности компьютера



Вирусы и программычерви

Программы, проникающие в компьютер для копирования, повреждения или уничтожения данных.



Программытрояны

Вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных сведений.



Программы-шпионы

Программы, отслеживающие ваши действия в Интернете или отображающие навязчивую рекламу.

Основные угрозы безопасности детей в Интернете



Киберхулиганы

И дети, и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей.



Злоупотребление общим доступом к файлам

Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ.



Хищники

Эти люди используют Интернет для того, чтобы заманить детей на личную встречу.



Если дети используют Интернет без присмотра, они могут столкнуться с изображениями или информацией, от которой их желательно оградить.

Вторжение в частную жизнь

Заполняя различные формы в Интернете, дети могут оставить конфиденциальные сведения о себе или свой семье.

Основные угрозы личной безопасности в Интернете



Фишинг

Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить вас посетить поддельные вебузлы и предоставить личные сведения



Нежелательная почта

Нежелательные сообщения элект-ронной почты, мгновенные сообщения и другие виды коммуникации

Кража идентификационных сведений

Преступление, связанное с похищением личных сведений и получением доступа к наличным деньгам или кредиту

Мистификация

Сообщения электронной почты, отправленные, чтобы обманом вынудить пользователя отдать деньги

Что вы можете предпринять



Ваш компьютер

- Включите интернетбрандмауэр Windows.
- Используйте Центр обновления Microsoft для автоматической загрузки новейших обновлений Windows.
- Установите и регулярно обновляйте антивирусное программное обеспечение.
- Установите и регулярно обновляйте Защитник Windows (Microsoft Windows Defender)



Ваша семья

- Поговорите с детьми о том, что они делают в Интернете.
- Установите четкие правила использования Интернета.
- Держите личные сведения в секрете.
- Используйте настройки семейной безопасности в программном обеспечении Microsoft.



Вы сами

- Выработайте линию поведения в Интернете, снижающую риски.
- Аккуратно обращайтесь с личными сведениями.
- Используйте технологии антифишинга и защиты от нежелательной почты, встроенные в Windows Vista, Windows XP SP2, Windows Live и Microsoft Outlook.

Включите интернет-брандмауэр Windows



Интернет-брандмауэр создает защитный барьер между вашим компьютером и Интернетом

Используйте автоматическое обновление для загрузки новейших обновлений программного обеспечения

- Устанавливайте все обновления, как только они становятся доступны
- Автоматическое обновление обеспечивает наилучшую защиту



Установите и регулярно обновляйте антивирусное программное обеспечение



- Антивирусное
 программное обеспечение
 помогает обнаруживать и
 удалять компьютерные
 вирусы, прежде чем они
 смогут навредить.
- Для эффективности антивирусного программного обеспечения регулярно обновляйте его.

Установите и регулярно обновляйте антишпионское программное обеспечение



Используйте антишпионское программное обеспечение, такое как Защитник Windows (Microsoft Windows Defender), чтобы неизвестные программы не могли отслеживать ваши действия в сети и похищать ваши сведения.

Другие способы защиты компьютера



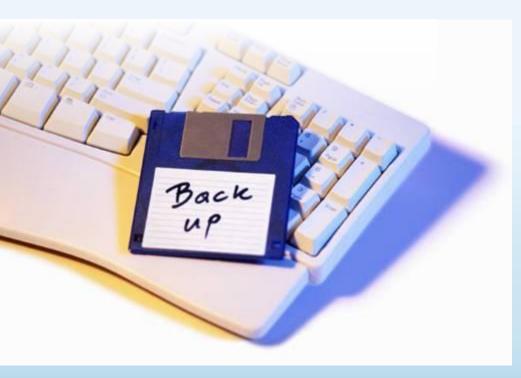
Архивируйте регулярно Ваши данные

Читайте заявления о конфиденциальности на веб-узлах

Закрывайте всплывающие окна при помощи красной кнопки «Х»

Думайте, прежде чем щелкать по ссылке

Архивируйте свои файлы



- Сохраняйте их на компакт- или DVD- дисках, USB- накопителях или других внешних носителях
- Используйте вебслужбы архивации

Думайте, прежде чем щелкать по ссылке

- Будьте осторожны с вложениями и ссылками в сообщениях электронной почты
- Загружайте файлы только с веб-узлов, которым доверяете

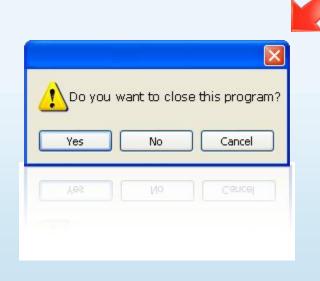


Изучайте заявления о конфиденциальности

Старайтесь понять, на что Вы соглашаетесь, прежде чем подтвердить отправку или предоставить личные сведения



Закрывайте всплывающие окна только щелчком по красной кнопке (X)



- Всегда используйте красную кнопку (X) в углу всплывающего окна.
- Никогда не нажимайте «Да», «Принять» и даже «Отмена», поскольку это может привести к установке программы на компьютер.

Действия, которые помогут защитить вашу семью

- **Поговорите** с детьми о том, что они делают в Интернете
- **Установите** четкие правила использования Интернета
- 3 Держите личные сведения в секрете
- **Используйте** программные продукты для обеспечения семейной безопасности

Обсудите с детьми опасности Интернета

- Открыто поговорите с детьми об опасностях Интернета, в том числе и о следующем.
 - Интернет-преступники
 - Недопустимый контент
 - Вторжение в частную жизнь
- Объясните им, как их собственное поведение может снизить угрозу и обеспечить безопасность в Интернете



Уделите внимание тому, чем дети занимаются в Интернете

- Держите компьютер в центре внимания
- Узнайте, для чего
 Ваши дети используют
 Интернет
- Позвольте Вашим детям учить Вас
- Научите их доверять своим инстинктам
- Убедите их сообщать о любых неприятностях



Держите личные сведения в секрете

- Научите детей советоваться с Вами, прежде чем предоставить личные сведения в Интернете
- Следите за деятельностью детей в Интернете
- Научите детей сообщать Вам о подозрительных действиях
- Помогите детям выбрать подходящие псевдонимы и адреса электронной почты



Установите четкие правила использования Интернета

- Не открывайте файлы для общего доступа и не открывайте вложения
- Не щелкайте по ссылкам в сообщениях электронной почты
- Относитесь к другим так, как хотите, чтобы относились к вам
- Защищайте себя
- Уважайте собственность других людей
- Никогда не отправляйтесь на личную встречу с «другом» из Интернета



Используйте программы для обеспечения семейной безопасности

- Эта возможность доступна в Windows Vista®, Windows Live™
 OneCare™ Family Safety и Xbox 360®
- Помогает родителям управлять контентом, который просматривают дети, а также быть в курсе того, чем они занимаются и с кем общаются в Интернете



Действия, которые помогут защитить ваши личные сведения

- **Выработайте** линию поведения в Интернете, снижающую риски для вашей безопасности
- **Обращайтесь** с личными сведениями аккуратно
- **Используйте** технологии для снижения рисков и при необходимости поднимайте тревогу

Выработайте линию поведения в Интернете, снижающую риски для вашей безопасности



- Удаляйте нежелательную почту, не открывая ее
- Остерегайтесь мошенничества в Интернете
- Используйте надежные пароли

Все говорят, что нельзя в качестве пароля использовать кличку собаки. Не знаю, а мне нравится, как зовут мою собаку:

!gA4=u6\$rU%

Осторожно обращайтесь с личными сведениями



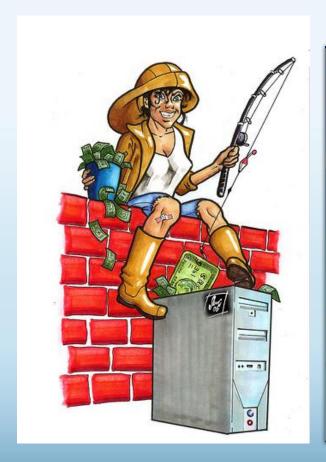
- Никогда не сообщайте личные сведения в мгновенных сообщениях или электронной почте
- Пользуйтесь только безопасными и надежными веб-узлами
- Убедитесь, что Вы попали именно туда, куда намеревались: веб-узлы могут быть поддельными
- Избегайте финансовых операций по беспроводным сетям
- В публичном месте сохраняйте конфиденциальность

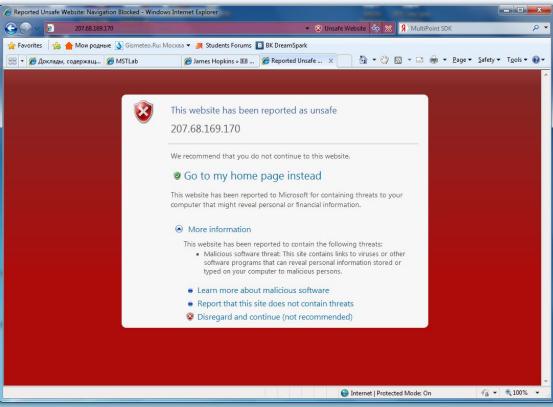
Пользуйтесь технологиями антифишинга и защиты от нежелательной почты

- Множество поставщиков электронной почты, а также такие программы, как Windows Live Hotmail® и Microsoft Outlook®, отфильтровывают большинство сообщений с нежелательной почтой
- Антифишинг в Internet Explorer® блокирует и предупреждает о подозрительных веб-узлах



Пользуйтесь технологиями антифишинга и защиты от нежелательной почты





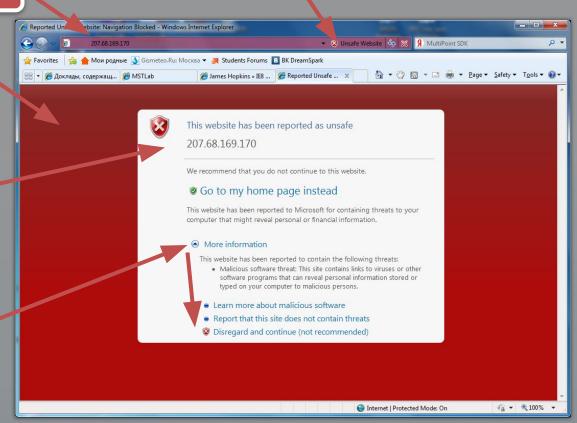


Подсветка домена

Красный фон

Предупреждение на странице

<u>Дополнительные</u> действия для продолжения



Если Ваши идентификационные сведения похищены

- Сообщите об этом
- Ведите записи
- Измените все пароли
- Заявите о мошенничестве в кредитных отчетах

Получите копию **кредитного отчета** и убедитесь, что ваш счет отмечен записями «Мошенничество» и «Заявление пострадавшего»

Как Microsoft укрепляет защиту и безопасность?



Сотрудничество

Сотрудничество с общественными организациями, технологическими компаниями и правительствами по всему миру для обеспечения безопасности в Интернете.



Технологии

Разработка программных продуктов и средств повышения защиты и безопасности помогает снизить риски Интернета и сделать обдуманный выбор.



Руководства

Предоставление полезных руководств, помогающих узнать об опасностях в Интернете и о том, как им противостоять.

Дополнительные источники

