Памятка "Компьютерная безопасность"

Компьютерная безопасность:
как оградить своего ребёнка от киберпреступников

Развитие в Республике Беларусь электронных технологий и телекоммуникационных сетей, всеобщая доступность в глобальной компьютерной сети Интернет различных информационных ресурсов способствовало появлению принципиально нового вида нарушения Закона – киберпреступности.

Киберпреступность – незаконные действия, которые осуществляются людьми, использующими информационные технологии для преступных целей.

Практика последних лет свидетельствует об увеличении числа таких преступлений, совершаемых несовершеннолетними. За 2015-ый год по Республике с участием несовершеннолетних зарегистрировано 38 хищений путем использования компьютерной техники (статья 212 УК Республики Беларусь).

Наиболее распространенными преступлениями в сфере компьютерной информации являются блокирование сайтов и локальных компьютерных сетей, незаконное копирование информации.

С учетом данной негативной тенденции уголовно-правовые нормы, касающиеся указанной категории правонарушителей, постоянно совершенствуются, в том числе путем снижения возраста, с которого наступает уголовная ответственность.Закон Республики Беларусь от 5-го января 2015-го года “О внесении изменений и дополнений в некоторые кодексы Республики Беларусь” с 4-го апреля 2016-го года снижен возраст лиц, с 16-ти до 14-ти лет, подлежащих ответственности по статье 212 УК Республики Беларусь (“Хищение путем использования компьютерной техники либо введения в компьютерную систему ложной информации”; наказание – вплоть до лишения свободы на срок до 3-х лет) а также по статье 349 Уголовного кодекса (“Несанкционированный доступ к компьютерной информации, совершенный из корыстной или иной личной заинтересованности, либо группой лиц”; наказывается на срок до 2-х лет лишения свободы, а повлекший по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми или иные тяжкие последствия – на срок до 7-ми лет.

Уважаемые родители, хотелось бы напомнить:

- предостерегайте детей от использования сети Интернет в хулиганских целях;
- приучайте их посещать только те сайты, которые Вы разрешили;
- настаивайте на том, чтобы дети никогда не соглашались на личную встречу с друзьями из Интернета без Вашего согласия;
- убеждайтесь, что ребенок советуется с Вами перед покупкой или продажей чего-либо посредством сети Интернет;
- контролируйте, какими чатами и досками объявлений пользуются Ваши дети;
- не разрешайте им открывать письма от неизвестных пользователей;
- приучите ребят спрашивать разрешения при скачивании программ или файлов из Интернета;
- напоминайте детям о конфиденциальности личной информации, объясните, к чему ее разглашение может привести.

Защита детей в Интернете: что могут сделать взрослые?

- Объясните детям и установите четкие правила – какие сайты они не должны посещать.
- Помогите детям выбрать правильное регистрационное имя и пароль, если это необходимо для общения детей посредством программ мгновенного обмена сообщениями или сетевых игр. Убедитесь в том, что они не содержат никакой личной информации.
- Объясните вашим детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.
- Объясните детям, что люди в Интернете не всегда являются теми, за кого они себя выдают. Не позволяйте детям встречаться лично с их «знакомыми» по Интернету без вашего наблюдения.
- Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.
- Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.
- Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости.
- Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты посещает ребенок и с какой целью. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь.
- Поощряйте детей делиться с вами их опытом в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет-дневник, регулярно посещайте его.

Будьте внимательны к вашим детям!

Возрастные особенности детей и Интернет

Ребенок проходит в своем психологическом развитии определенные стадии, которые достаточно сильно отличаются друг от друга. Это также отражается и на интересах детей при пользовании Интернетом. Родителям важно понимать особенности формирования их характера и интересы в том или ином возрасте, для того чтобы правильно расставлять акценты внимания при своих беседах с детьми о правилах безопасности в Интернете.

Более подробную информацию по повышению безопасности детей различного возраста в Интернете см. на веб-сайте Microsoft по адресу http://www.microsoft.com/rus/athome/security/children/parentsguide.mspx

Повышение уровня безопасности детей в Интернете при помощи программных средств

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. Пожалуйста, примите необходимые меры, чтобы защитить ваших детей при помощи программных средств. Но помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

- Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам (например, с помощью Internet Explorer®)
- Увеличьте уровень защиты и конфиденциальности:
  - используя возможности Microsoft® Windows XP, создайте отдельные учетные записи для разных пользователей
  - настройте параметры безопасности Internet Explorer®
- Следите за тем, какие сайты посещают ваши дети (например, с помощью Internet Explorer®)
- Напоминайте детям, чтобы они не общались в Интернете с незнакомцами. Помогите им оградить себя от неизвестных контактов (например, с помощью Microsoft Windows Messenger)

Более подробную информацию по повышению безопасности в Интернете с помощью технологических средств см. на веб-сайте Microsoft по адресу http://www.microsoft.com/rus/athome/security/children/childrenonline.mspx

РЕБЕНОК В ИНТЕРНЕТЕ. ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ

Предупредите ребёнка о том, что в Сети он может встретиться с опасным контентом. Об этом нужно рассказать родителям.

Расскажите ребёнку о мошенничестве в Сети, лотереях, розыгрышах.

Договоритесь с ребенком сколько времени он будет проводить в Интернете. Для каждого возраста должна быть своя норма - чем старше ребенок, тем дольше он может находиться в Сети

Приучите детей, что нельзя раскрывать свои личные данные в Интернете.
если майт требует ввода имени, помогите ребенку придумать псевдоним, нераскрывающий никакой личной информации.

Беседуйте с детьми об их виртуальных друзьях. Если ребенок хочет встретиться с Интернет-другом, то перед этим он обязательно должен посоветоваться с родителями.

Объясните ребенку, что в Интеренете человек может быть не тем, за кого он себя выдаёт. 10-летний ребенок может оказаться 40-летним дядей.

ТВОЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

В Европе свыше 13 миллионов детей, как ты, регулярно пользуются Интернетом. Если ты ищешь информацию по своему домашнему заданию или только хочешь повеселиться, то Интернет – замечательное место, но ты должен знать об опасностях и следовать советам:

НЕ НАЖИМАЙ НЕИЗВЕСТНЫЕ ССЫЛКИ

Когда ты общаешься в чатах и интернет-пейджерах или получаешь письмо, никогда не нажимай непосредственно на ссылку. **ЕСЛИ ОНА ПРИШЛА ОТ НЕЗНАКОМОГО ЧЕЛОВЕКА, ЛУЧШЕ НЕ ОБРАЩАТЬ НА НЕЕ ВНИМАНИЯ.**

НЕ СКАЧИВАЙ ФАЙЛЫ ИЗ НЕИЗВЕСТНЫХ ИСТОЧНИКОВ

Без сомнения, ты часто получаешь сообщения, предлагающие тебе скачать фото, песню или видео. **ИНОГДА ТАКИЕ ФАЙЛЫ МОГУТ ОТПРАВЛЯТЬСЯ НЕ ЧЕЛОВЕКОМ ИЗ ТВОИХ КОНТАКТОВ, А ВИРУСОМ, КОТОРЫЙ ЗАРАЗИЛ ЕГО КОМПЬЮТЕР И ПЫТАЕТСЯ РАСПРОСТРАНИТЬСЯ СРЕДИ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ.**

Именно по этой причине ты должен всегда спрашивать своего знакомого, действительно ли он отправил тебе сообщение или файл. Если он этого не делал, сообщи ему, что его компьютер заражен. Пусть он сообщит своим знакомым, которые получили от него подобное сообщение или файл, чтобы они не открывали их и

НЕ ОТКРЫВАЙ ПОДОЗРИТЕЛЬНЫЕ ФАЙЛЫ

Если твое решение безопасности говорит тебе, что файл содержит или может содержать угрозу, не открывай файл. **ПРОСТО УДАЛИ ЕГО.**

НЕ ОБЩАЙСЯ С НЕЗНАКОМЦАМИ

В чатах или системах обмена мгновенными сообщениями **ТЫ НИКОГДА НЕ МОЖЕШЬ БЫТЬ УВЕРЕН В ТОМ, КТО С ТОБОЙ ОБЩАЕТСЯ.** Никогда не заводи дружбу с незнакомцами, и ни под какими предлогами не соглашайтесь на встречу с ними в реальной жизни.

НЕ РАСПРОСТРАНЯЙ В ИНТЕРНЕТЕ ЛИЧНУЮ ИНФОРМАЦИЮ

Никогда не отправляй свою личную информацию (твои данные, фотографии, адрес и пр.) по электронной почте и через системы обмена мгновенными сообщениями, а также никогда не публикуй такого рода информацию в блогах и форумах. Кроме того, будь внимательным при создании профилей в таких сервисах, как Facebook или MySpace.
Ты никогда не должен размещать такую конфиденциальную информацию, как твой возраст и твой адрес проживания. Также рекомендуем тебе не использовать свое настоящее имя, а пользоваться псевдонимом или ником.

ОСТЕРЕГАЙТЕСЬ ЗАМАНЧИВЫХ ПРЕДЛОЖЕНИЙ РАБОТЫ

Как правило, никто ничего не дает просто так. Если ты получил фантастическое предложение работы от неизвестных пользователей, то **НЕ ОБРАЩАЙ НА НЕГО ВНИМАНИЯ.**

БЕЗОПАСНОСТЬ в Интернете

Не указывай свою личную информацию, настоящее имя, адрес, телефон и места, где ты часто бываешь.

Относись с осторожностью к публикации личных фото. Не выкладывай фото других людей без их согласия.

Не доверяй всей информации, размещенной в Интернете. Не доверяй незнакомым людям, они могут выдавать себя за других.

Не переходи по сомнительным ссылкам (например, обещающим выигрыш). Не посещай сомнительные сайты. Они могут нанести вред твоей психике.

Помни, что незаконное копирование авторских материалов преследуется по закону.

Не встречайся в реальной жизни с людьми, с которыми ты познакомился в Интернете. Сообщи родителям, если друзья из Интернета настаивают на личной встрече.

Помни, что в виртуальном мире действуют те же правила вежливости, что и в реальном.

Не отправляй смс, чтобы получить какую-либо услугу или выиграть приз.

Обращайся за советом к взрослым при малейшем сомнении или подозрении.

Основные угрозы личной безопасности в Интернете

Фишинг
Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить вас посетить поддельные веб-узлы и предоставить личные сведения

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

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

Нежелательная почта
Нежелательные сообщения электронной почты, мгновенные сообщения и другие виды коммуникации

Основные угрозы безопасности компьютера

Вирусы и программы-черви
Программы, проникающие в компьютер для копирования, повреждения или уничтожения данных

Программы-трояны
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

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 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

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

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

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