Бежит по клавишам рука

И пальцы высекают слово:

Пока-привет, привет-пока -

Банальностями сыплем снова!

Какая магия влечет,

Сесть к монитору заставляет?

Но все быстрее кровь течет!

И к слову слово прибавляем.

Соединил нас Интернет,

Сквозь расстояния и годы,

Привет-пока, пока-привет…

Ну что? А как у вас погода?

Что нового? И как дела?

В семейной, ну и в жизни личной?

Что видел ты? Где ты была?

Все – класс! И у меня – отлично!

Сегодня мы не представляем свою жизнь без компьютера и сети

Интернет. В настоящее время ведется множество неоднозначных разговоров

о пользе и вреде всемирной сети. Дети и подростки - активные пользователи

интернета, ведь он предоставляет подрастающему поколению невероятные

возможности для совершения открытий, общения и творчества. Но у любого

явления есть свои светлые и темные стороны, и зачастую дети и молодежь в

полной мере не осознают все возможные проблемы, с которыми они могут

столкнуться в сети.

Интернет представляет собой открытое окно в мир, который также

принадлежит взрослым и содержит материалы, не подходящие для детей,

поэтому с использованием киберпространства связаны определенные риски.

Как должны родители и взрослые помочь детям избежать все

возможные неприятности, чтобы сделать их пребывание в интернете более

безопасным, научить их ориентироваться во всемирной сети? Простого

ответа не существует. Риски могут быть разными в зависимости от возраста и

компьютерной грамотности ребенка.

Конечно же, отказ от использования этих современных технологий не

является решением проблемы защиты детей в онлайн-пространстве. Это все

равно что запретить ездить автотранспорту по улицам и придворовым

территориям, чтобы дети не попадали в ДТП. Во избежание несчастных

случаев нужно лишь научить ребенка быть осторожным, соблюдать

определенные правила, быть ответственным пешеходом, следовать

положительному примеру взрослых. Аналогично наиболее важной задачей

взрослых является предупреждение детей об опасностях Интернета, чтобы

они вели себя осторожно, обдуманно. Кроме того, необходимо обсуждать с

детьми все те вопросы, которые могут у них возникнуть при использовании

Интернета.

4

На нашей встрече мы поговорим о возможных рисках, с которыми могут

столкнуться наши дети в интернете.

Итак, риск первый - это безопасность личной информации на

собственном компьютере, что означает защиту от вирусов, вредоносного

ПО и постоянное обновление программного обеспечения. Как защитить в

этом случае своих детей? Прежде всего, повысить уровень защиты данных.

Это можно сделать путем использования настроек фильтра и параметров

фильтрации содержимого, которые доступны во многих программах. Кроме

того, велика угроза заражения вредоносным ПО. Ведь для его

распространения и проникновения в компьютеры используется целый спектр

методов. Среди них можно отметить не только почту, компакт-диски,

дискеты и прочие сменные 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.

Этот метод часто используется хакерами для распространения троянских

вирусов. Дети, неискушенные в вопросах социальной инженерии, могут

легко попасться на уловки злоумышленника.

Чтобы избежать риска потерять личную информацию на компьютере,

нужно соблюдать достаточно простые правила безопасности:

• Регулярно обновляйте операционную систему.

• Используйте только лицензионные программы и данные, полученные

из надежных источников. Чаще всего вирусами бывают заражены

пиратские копии программ, особенно компьютерные игры.

• Используйте антивирусную программу, которая постоянно обновляет

свои базы, и еженедельно проверяйте компьютер на наличие вирусов.

• Создавайте резервные копии важных файлов, так называемые, "бэк-

апы" (например, на отдельном, только для этого и предназначенном

винчестере или usb-накопителе).

• Будьте осторожны при загрузке содержимого в Интернет. Помните:

после публикации информации во всемирной сети ее больше

невозможно будет контролировать и удалять каждую ее копию.

• Будьте внимательны при загрузке контента из Интернета: при

малейшем сомнении откажитесь от "закачки" данных на свой

компьютер.

• Старайтесь периодически менять пароли (например, от электронной

почты, от профилей в социальных сетях), но не используйте слишком

простые пароли, которые можно легко взломать (даты рождения,

номера телефонов и т.п). Никому не сообщайте пароли!

• При пользовании интернетом на чужом устройстве, не сохраняйте

пароли и не забывайте выходить из своего аккаунта в социальной сети,

в почте и на других сайтах после завершения работы.

• Объясните все эти правила своим детям!

 Осторожно. Кибератака!!!

Вас беспокоит ситуация с киберпреступностью? Понимание того, что такое киберпреступение, какие типы киберпреступлений существуют и как от них защититься, поможет вам чувствовать себя увереннее.

В этой статье мы подробно расскажем о том, что такое киберпреступность, от каких угроз и как нужно защищаться, чтобы обеспечить свою безопасности в Интернете. Мы затронем следующие темы:

* Что такое киберпреступность
* Типы киберпреступлений
* Что считается киберпреступлением (на примерах)
* Как защититься от киберпреступников

**Что такое киберпреступление**

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство (но не все) киберпреступления совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией. Другие – начинающие хакеры.

Киберпреступники редко взламывают компьютеры по причинам, не имеющим отношения к получению прибыли, например, по политическим или личным.

**Типы киберпреступлений**

Вот несколько примеров различных тиров киберпреступлений:

* Мошенничество с электронной почтой и интернет-мошенничество
* Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации)
* Кража финансовых данных или данных банковских карт
* Кража и продажа корпоративных данных
* Кибершантаж (требование денег для предотвращения кибератаки)
* Атаки программ-вымогателей (тип кибершантажа)
* Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
* Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Большинство киберпреступлений относится к одной из двух категорий

* Криминальная деятельность, целью которой являются сами компьютеры
* Криминальная деятельность, в которой компьютеры используются для совершения других преступлений

В первом случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью зловредов можно удалять или похищать данные.

Киберпреступления, в результате которых владельцы устройств не могут пользоваться своими компьютерами или сетью, а компании - предоставлять интернет-услуги своим клиентам, называется атакой отказа в обслуживании (DoS).

Киберпреступления второй категории используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений.

Иногда злоумышленники могут совмещать обе категории киберпреступлений. Сначала они заражают компьютеры с вирусами, а затем используют их для распространения вредоносного ПО на другие машины или по всей сети.

Киберпреступники могут также выполнять так называемую атаку с распределенным отказом в обслуживании (DDos). Она похожа на DoS-атаку, но для ее проведения преступники используют множество скомпрометированных компьютеров.

Министерство юстиции США считает, что есть еще и третья категория киберпреступлений, когда компьютер используется как соучастник незаконного деяния, например, для хранения на нем украденных данных.

США подписали [Европейскую конвенцию о киберпреступности](https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185). В ней названы виды деятельности с использованием компьютеров, которые считаются киберпреступлениями. Например:

* незаконный перехват или кража данных.
* компрометация компьютерных систем и сетей
* нарушение авторских прав
* незаконные азартные игры
* продажа запрещенных предметов в Интернете
* домогательство, производство или хранение детской порнографии

## Примеры киберпреступлений

Итак, что именно считается киберпреступлением?

В этом разделе мы рассмотрим резонансные примеры различных типов кибератак.

### Атаки с использованием вредоносного ПО

Атака с использованием вредоносного ПО - это заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО.

Компьютер, зараженный вредоносной программой, может использоваться злоумышленниками для достижения разных целей. К ним относятся кража конфиденциальных данных, использование компьютера для совершения других преступных действий или нанесение ущерба данным.

Известным примером атаки с использованием вредоносного ПО является атака вымогателя WannaCry, случившаяся в мае 2017 года.

Ransomware - это тип вредоносного ПО, который используется для получения денег в обмен на разблокирование устройства/файлов жертвы. WannaCry - это тип программ-вымогателей, которые используют уязвимость компьютеров Windows.

Жертвами WannaCry стали 230 000 компьютеров в 150 странах мира. Владельцы заблокированных файлов отправили сообщение с согласием заплатить выкуп в криптовалюте BitCoin за восстановление доступа к своим данным.

Финансовые потери в результате деятельности WannaCry оцениваются в 4 миллиарда долларов.

### Фишинг

Фишинговая кампания - это массовая рассылка спам-сообщений или других форм коммуникации с целью заставить получателей выполнить действия, которые ставят под угрозу их личную безопасность или безопасность организации, в которой они работают.

Сообщения в фишинговой рассылке могут содержать зараженные вложения или ссылки на вредоносные сайты. Они также могут просить получателя в ответном письме предоставить конфиденциальную информацию.

Известный пример фишинг-мошенничества году произошел на Чемпионате мира по футболу в 2018. [По информации Inc](https://www.inc.com/will-yakowicz/biggest-email-phishing-scams-2018.html), фишинговые электронные письма рассылались футбольным фанатам.

В этих письмах злоумышленники соблазняли болельщиков фальшивыми бесплатными поездками в Москву на Чемпионат мира. У людей, которые проходили по ссылке в сообщениях, были украдены личные данные.

Другой тип фишинговой кампании известен как целевой фишинг. Мошенники пытаются обмануть конкретных людей, ставя под угрозу безопасность организации, в которой они работают.

В отличие от массовых неперсонифицированных фишинговых рассылок сообщения для целевого фишинга создаются так, чтобы у получателя не возникло сомнений, что они отправлены из надежного источника, например, от генерального директора или IT-менеджера.

### Распределённые атаки типа «отказ в обслуживании»

Распределенные типа «отказ в обслуживании» (DDoS) - это тип кибератаки, которую злоумышленники используют для взлома системы или сети. Иногда для запуска DDoS-атак используются подключенные устройства IoT (Интернет вещей).

DDoS-атака перегружает систему большим количеством запросов на подключение, которые она рассылает через один из стандартных протоколов связи.

Кибершантажисты могут использовать угрозу DDoS-атаки для получения денег. Кроме того, DDoS запускают в качестве отвлекающего маневра в момент совершения другого типа киберпреступления.

Известным примером DDoS-атаки является [атака на веб-сайт Национальной лотереи Великобритании 2017 году](https://www.welivesecurity.com/2017/10/02/uk-national-lottery-ddos-attack/). Результатом стало отключение веб-сайта и мобильного приложения лотереи, что не позволило гражданам Великобритании играть.

## Как не стать жертвой киберпреступления

Итак, теперь, когда вы понимаете, какую угрозу представляет киберпреступность, встает вопрос о том, как наилучшим образом защитить ваш компьютер и личные данные? Следуйте нашим советам:

### Регулярно обновляйте ПО и операционную систему

Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.

### Установите антивирусное ПО и регулярно его обновляйте

Использование антивируса или комплексного решения для обеспечения интернет-безопасности, такого как [Kaspersky Total Security](https://www.kaspersky.ru/total-security), - это правильный способ защитить вашу систему от атак.

Антивирусное ПО позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Оно помогает защитить ваш компьютер и ваши данные от киберпреступников.

Если вы используете антивирусное программное обеспечение, регулярно обновляйте его, чтобы обеспечить наилучший уровень защиты.

### Используйте сильные пароли

Используйте сильные пароли, которые трудно подобрать, и нигде их не записывайте. Можно воспользоваться услугой надежного менеджера паролей, который облегчит вам задачу, предложив сгенерированный им сильный пароль.

### Не открывайте вложения в электронных спам-сообщениях

Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений - это вложения в электронных спам-сообщениях. Никогда не открывайте вложение от неизвестного вам отправителя.

### Не нажимайте на ссылки в электронных спам-сообщениях и не сайтах, которым не доверяете

Еще один способ, используемый киберпреступниками для заражения компьютеров пользователей, - это вредоносные ссылки в спамовых электронных письмах или других сообщения, а также на незнакомых веб-сайтах. Не проходите по этим ссылкам, чтобы не стать жертвой интернет-мошенников.

### Не предоставляйте личную информацию, не убедившись в безопасности канала передачи

Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонное соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.

### Свяжитесь напрямую с компанией, если вы получили подозрительный запрос

Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте, и убедитесь, что вам звонили не мошенники.

Желательно пользоваться, при этом, другим телефоном, потому что злоумышленники могут оставаться на линии: вы будете думать, что набрали номер заново, а они будут отвечать якобы от имени банка или другой организации, с которой, по вашему мнению, вы разговариваете.

### Внимательно проверяйте адреса веб-сайтов, которые вы посещаете

Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Они выглядят легитимно? Не переходить по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса.

Если ваш продукт для обеспечения безопасности в Интернете включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

### Внимательно просматривайте свои банковские выписки

Наши советы должны помочь вам не стать жертвой киберпреступников. Но если все же это случилось, важно понять, когда это произошло.

Просматривайте внимательно свои банковские выписки и запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.

Теперь вы понимаете, какую угрозу представляют киберпреступники, и знаете, как от нее защититься.

5

Риск второй - разглашение контактных данных.

В Интернете (чатах, социальных сетях и т.п.) дети могут общаться с

другими детьми и заводить новых друзей, что подразумевает обмен

определенной личной информацией, по которой можно установить личность

ребенка, контактную информацию (полное имя, почтовый адрес и номер

телефона), подробности его быта, режима дня и и т.д. Личность человека

можно также установить, связав различные типы предоставленных данных

(например, название школы, спортивного клуба, места проживания и т.д.).

Подобная информация может быть использована в преступных целях.

Поэтому, давая положительный пример своим детям, старайтесь сами

соблюдать осторожность при разглашении контактных данных или другой

личной информации. Любые отправляемые фотографии или раскрываемые

незнакомцу личные сведения могут стать общедоступными в Интернете.

Интерактивные дневники могут надолго стать доступными для прочтения

широкой общественностью. После публикации в Интернете текста или

фотографии их невозможно контролировать. Их можно легко скопировать во

множество разных мест, и их полное удаление может оказаться

невозможным.

Соблюдайте правила безопасности вместе с детьми, обсуждая их

необходимость:

• Обговорите с детьми возможные опасные последствия предоставления

личной информации и те ситуации, когда рекомендуется скрывать

личную информацию (с учетом возраста и психологической

уравновешенности каждого ребенка).

• Помните: никогда не следует сообщать пароли никому, даже давним

друзьям. Кроме того, пароль необходимо регулярно менять. Научите

этому своих детей.

• Интернет является общественным местом. Перед публикацией любой

информации или своих фотографий (а также фотографий других

людей) следует помнить, что любой человек в мире сможет получить

доступ к этой информации.

• Ребенок должен знать, что в любой момент может поговорить с

родителями об отрицательном опыте, полученном в Интернете,

понимая, что получит поддержку и помощь от взрослых, а не

порицание и наказание.

Риск третий - это доступ к нежелательному содержимому.

Это может быть насилие, наркотики, порнография, страницы,

подталкивающие к самоубийствам, отказу 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.

6

Такая информация часто бывает заманчивой и может оказывать сильное

психологическое давление на детей и подростков, которые не способны до

конца осознать смысл происходящего и отказаться от просмотра и изучения

сайтов с подобным содержимым. Влияние подобного рода информации на

еще неокрепшую психику детей и подростков непредсказуемо; под

впечатлением от таких сайтов дети могут пострадать не только в

эмоциональном плане, но также прямой урон может быть нанесен и их

физическому здоровью.

Уберечь детей от данной нежелательной информации поможет

настройка контентной фильтрации с помощью дополнительных функций

антивирусных программ, интернет-браузеров или установки специального

программного обеспечения, например, Родительского контроля в Windows

Vista или средств Родительского контроля, встроенных в Kaspersky Internet

Надеюсь, сегодняшняя беседа поможет вам чувствовать себя а

безопасности на просторах интернета и помогать своим детям избегать

неприятностей в киберпространстве.

Спасибо за внимание!

Бежит по клавишам рука

И пальцы высекают слово:

Пока-привет, привет-пока -

Банальностями сыплем снова!

Какая магия влечет,

Сесть к монитору заставляет?

Но все быстрее кровь течет!

И к слову слово прибавляем.

Соединил нас Интернет,

Сквозь расстояния и годы,

Привет-пока, пока-привет…

Ну что? А как у вас погода?

Что нового? И как дела?

В семейной, ну и в жизни личной?

Что видел ты? Где ты была?

Все – класс! И у меня – отлично!

Сегодня мы не представляем свою жизнь без компьютера и сети

Интернет. В настоящее время ведется множество неоднозначных разговоров

о пользе и вреде всемирной сети. Дети и подростки - активные пользователи

интернета, ведь он предоставляет подрастающему поколению невероятные

возможности для совершения открытий, общения и творчества. Но у любого

явления есть свои светлые и темные стороны, и зачастую дети и молодежь в

полной мере не осознают все возможные проблемы, с которыми они могут

столкнуться в сети.

Интернет представляет собой открытое окно в мир, который также

принадлежит взрослым и содержит материалы, не подходящие для детей,

поэтому с использованием киберпространства связаны определенные риски.

Как должны родители и взрослые помочь детям избежать все

возможные неприятности, чтобы сделать их пребывание в интернете более

безопасным, научить их ориентироваться во всемирной сети? Простого

ответа не существует. Риски могут быть разными в зависимости от возраста и

компьютерной грамотности ребенка.

Конечно же, отказ от использования этих современных технологий не

является решением проблемы защиты детей в онлайн-пространстве. Это все

равно что запретить ездить автотранспорту по улицам и придворовым

территориям, чтобы дети не попадали в ДТП. Во избежание несчастных

случаев нужно лишь научить ребенка быть осторожным, соблюдать

определенные правила, быть ответственным пешеходом, следовать

положительному примеру взрослых. Аналогично наиболее важной задачей

взрослых является предупреждение детей об опасностях Интернета, чтобы

они вели себя осторожно, обдуманно. Кроме того, необходимо обсуждать с

детьми все те вопросы, которые могут у них возникнуть при использовании

Интернета.

4

На нашей встрече мы поговорим о возможных рисках, с которыми могут

столкнуться наши дети в интернете.

Итак, риск первый - это безопасность личной информации на

собственном компьютере, что означает защиту от вирусов, вредоносного

ПО и постоянное обновление программного обеспечения. Как защитить в

этом случае своих детей? Прежде всего, повысить уровень защиты данных.

Это можно сделать путем использования настроек фильтра и параметров

фильтрации содержимого, которые доступны во многих программах. Кроме

того, велика угроза заражения вредоносным ПО. Ведь для его

распространения и проникновения в компьютеры используется целый спектр

методов. Среди них можно отметить не только почту, компакт-диски,

дискеты и прочие сменные 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.

Этот метод часто используется хакерами для распространения троянских

вирусов. Дети, неискушенные в вопросах социальной инженерии, могут

легко попасться на уловки злоумышленника.

Чтобы избежать риска потерять личную информацию на компьютере,

нужно соблюдать достаточно простые правила безопасности:

• Регулярно обновляйте операционную систему.

• Используйте только лицензионные программы и данные, полученные

из надежных источников. Чаще всего вирусами бывают заражены

пиратские копии программ, особенно компьютерные игры.

• Используйте антивирусную программу, которая постоянно обновляет

свои базы, и еженедельно проверяйте компьютер на наличие вирусов.

• Создавайте резервные копии важных файлов, так называемые, "бэк-

апы" (например, на отдельном, только для этого и предназначенном

винчестере или usb-накопителе).

• Будьте осторожны при загрузке содержимого в Интернет. Помните:

после публикации информации во всемирной сети ее больше

невозможно будет контролировать и удалять каждую ее копию.

• Будьте внимательны при загрузке контента из Интернета: при

малейшем сомнении откажитесь от "закачки" данных на свой

компьютер.

• Старайтесь периодически менять пароли (например, от электронной

почты, от профилей в социальных сетях), но не используйте слишком

простые пароли, которые можно легко взломать (даты рождения,

номера телефонов и т.п). Никому не сообщайте пароли!

• При пользовании интернетом на чужом устройстве, не сохраняйте

пароли и не забывайте выходить из своего аккаунта в социальной сети,

в почте и на других сайтах после завершения работы.

• Объясните все эти правила своим детям!

5

Риск второй - разглашение контактных данных.

В Интернете (чатах, социальных сетях и т.п.) дети могут общаться с

другими детьми и заводить новых друзей, что подразумевает обмен

определенной личной информацией, по которой можно установить личность

ребенка, контактную информацию (полное имя, почтовый адрес и номер

телефона), подробности его быта, режима дня и и т.д. Личность человека

можно также установить, связав различные типы предоставленных данных

(например, название школы, спортивного клуба, места проживания и т.д.).

Подобная информация может быть использована в преступных целях.

Поэтому, давая положительный пример своим детям, старайтесь сами

соблюдать осторожность при разглашении контактных данных или другой

личной информации. Любые отправляемые фотографии или раскрываемые

незнакомцу личные сведения могут стать общедоступными в Интернете.

Интерактивные дневники могут надолго стать доступными для прочтения

широкой общественностью. После публикации в Интернете текста или

фотографии их невозможно контролировать. Их можно легко скопировать во

множество разных мест, и их полное удаление может оказаться

невозможным.

Соблюдайте правила безопасности вместе с детьми, обсуждая их

необходимость:

• Обговорите с детьми возможные опасные последствия предоставления

личной информации и те ситуации, когда рекомендуется скрывать

личную информацию (с учетом возраста и психологической

уравновешенности каждого ребенка).

• Помните: никогда не следует сообщать пароли никому, даже давним

друзьям. Кроме того, пароль необходимо регулярно менять. Научите

этому своих детей.

• Интернет является общественным местом. Перед публикацией любой

информации или своих фотографий (а также фотографий других

людей) следует помнить, что любой человек в мире сможет получить

доступ к этой информации.

• Ребенок должен знать, что в любой момент может поговорить с

родителями об отрицательном опыте, полученном в Интернете,

понимая, что получит поддержку и помощь от взрослых, а не

порицание и наказание.

Риск третий - это доступ к нежелательному содержимому.

Это может быть насилие, наркотики, порнография, страницы,

подталкивающие к самоубийствам, отказу 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.

6

Такая информация часто бывает заманчивой и может оказывать сильное

психологическое давление на детей и подростков, которые не способны до

конца осознать смысл происходящего и отказаться от просмотра и изучения

сайтов с подобным содержимым. Влияние подобного рода информации на

еще неокрепшую психику детей и подростков непредсказуемо; под

впечатлением от таких сайтов дети могут пострадать не только в

эмоциональном плане, но также прямой урон может быть нанесен и их

физическому здоровью.

Уберечь детей от данной нежелательной информации поможет

настройка контентной фильтрации с помощью дополнительных функций

антивирусных программ, интернет-браузеров или установки специального

программного обеспечения, например, Родительского контроля в Windows

Vista или средств Родительского контроля, встроенных в Kaspersky Internet

Если компьютером пользуются и взрослые, то для ребенка лучше

создать отдельную учетную запись пользователя, в которой настраивается

фильтрация и родительский контроль. При этом вы будете выполнять

функции администратора (отдельная учетная запись): вы сможете

контролировать системные настройки и устанавливать новое программное

обеспечение, ограничивая в таких правах других пользователей компьютера.

Не забывайте создавать для работы надежные и защищенные пароли.

Нежелательную. информацию можно получить и по электронной почте,

поэтому важно настроить почтовый ящик ребенка с помощью фильтрации

спама и таким образом предотвратить получение большей части

нежелательных сообщений. Еще один безопасный, хотя и очень

ограниченный способ использования электронной почты — это настроить

параметры так, чтобы ребенок получал сообщения только от указанных

адресов. Многие программы электронной почты позволяют блокировать

сообщения, отправляемые с определенных адресов электронной почты.

Риск четвертый - контакты с незнакомыми людьми. С подобными

рисками можно столкнуться при общении в чатах, онлайн-мессенджерах

(ICQ, Skype, MSN и др.), социальных сетях, на сайтах знакомств, форумах,

блогах и т.д. Примерами таких коммуникационных рисков могут быть:

кибербуллинг, незаконные контакты (например, груминг), знакомства в сети

и встречи с интернет-знакомыми и др.

Для детей и молодежи Интернет главным образом является социальной

средой, в которой можно не только встречаться с друзьями, но и с

незнакомцами. В Интернете пользователя могут обидеть, запугать или даже

оскорбить. С появлением киберпространства набирает обороты такое

явление, как кибербуллинг (bullying,от bully – драчун, задира, грубиян,

насильник), обозначающее запугивание, унижение, травлю, физический или

психологический террор, осуществляемый в виртуальной среде с помощью

интернета и мобильного телефона и направленный на то, чтобы вызвать у

7

другого страх и тем самым подчинить его себе. Запугивание в школе обычно

заканчивается вместе с занятиями, но в Интернете обидчик может настигнуть

свою жертву в любое время. Ведь запугивание или оскорбление в Интернете

легко осуществимо с технической точки зрения: для отправки

злонамеренного сообщения или публикации оскорбительного текста,

доступного широкой аудитории, требуется несколько щелчков мышью. К

тому же, в отличие от реального мира, виртуальность дает возможность

анонимности и обеспечивает низкую вероятность наказания.

Основной площадкой для кибербуллинга в последнее время являются

социальные сети. В них можно оскорблять человека не только с помощью

сообщений – нередки случаи, когда страницу жертвы взламывают (или

создают поддельную на ее имя), где размещают лживый и унизительный

контент.

И зачастую дети полагают, что если сообщить об этом родителям, это

только усугубит ситуацию, что в итоге поддерживает ситуацию запугивания.

Даже если ребенок не сталкивался с оскорблениями в Интернете, но ему

нравится общаться через Интернет, такие риски необходимо обсудить

заранее и ему необходимо дать совет относительно действий, которые

следует предпринять при причинении беспокойства. Прежде всего, ребенок

должен понимать, что в Интернете, как и в реальной жизни, каждый человек

имеет право на уважительное отношение, поэтому запрещается клеветать или

оскорблять других пользователей. Объясните детям, что при общении в

интернете они должны быть дружелюбными с другими пользователями. Ни в

коем случае не стоит писать резкие и оскорбительные слова – читать

грубости так же неприятно, как и слышать. Некоторые действия, для которых

потребовалось несколько щелчков мыши, очень сложно отменить, и дети

могут не понять, насколько серьезной может стать ситуация. А ведь при

необходимости анонимных пользователей можно отследить.

В случае, если ваш ребенок лично столкнулся с "негативным

собеседником", нужно объяснить, что общение можно прервать, закрыв чат,

клиент электронной почты или даже выключив компьютер. Возможно стоит

вообще покинуть данный ресурс, удали оттуда свою личную информацию,

если не получается решить проблему мирным путем. Ребенок должен понять,

что общение с подобными людьми нельзя продолжать (читать и отвечать на

оскорбительные сообщения и письма), но тем не менее, если злонамеренные

сообщения являются нарушением закона (преступлением против личности),

то их необходимо сохранить и показать взрослым. Кроме того, можно

настроить параметры программы работы с электронной почтой так, чтобы

сообщения от определенного отправителя поступали в отдельную папку. В

этом случае ребенку не придется их читать, а у вас будет достаточно

материалов для дальнейших действий. Если же вы сами обнаружили

материалы, оскорбляющие вас или ваших детей, обратитесь к

администратору сайта (модератору чата), чтобы данную информацию

удалили. Если же такового не произошло или администратор вам отказал в

8

удалении, то сохраните скриншоты переписки с ним и всех страниц с

оскорбительной информацией и обратитесь в полицию.

Особенно опасным риском является груминг – установление дружеских

отношений с ребенком с целью личной встречи, вступления с ним в

сексуальные отношения, шантажа и эксплуатации.

Для защиты детей от подобного риска необходимо соблюсти некоторые

правила:

• Поддерживайте доверительные отношения с вашим ребенком, чтобы

всегда быть в курсе, с кем ребенок общается в сети. Обратите

внимание, кого ребенок добавляет к себе «в друзья», с кем

предпочитает общаться в сети – с ровесниками или людьми старше

себя.

• Объясните ребенку, что нельзя разглашать в интернете информацию

личного характера (номер телефона, домашний адрес, название/номер

школы и т. д.), а также пересылать виртуальным знакомым свои

фотографии или видео.

• Объясните ребенку, что при общении на ресурсах, требующих

регистрации (в чатах, на форумах, через сервисы мгновенного обмена

сообщениями, в онлайн-играх), лучше не использовать реальное имя.

Помогите ему выбрать ник, не содержащий никакой личной

информации.

• Объясните ребенку опасность встречи с незнакомыми людьми из

интернета. В сети человек может представиться кем угодно, поэтому на

реальную встречу с интернет-другом надо обязательно ходить в

сопровождении взрослых.

• Детскийпознавательный интерес к теме сексуальных отношений между

мужчиной и женщиной может активно эксплуатироваться

злоумышленниками в интернете. Постарайтесь сами поговорить с

ребенком на эту тему. Объясните ему, что нормальные отношения

между людьми связаны с доверием, ответственностью и заботой, но в

интернете тема любви часто представляется в неправильной,

вульгарной форме.

• Важно, чтобы ребенок был вовлечен в любимое дело, увлекался

занятиями, соответствующими его возрасту, которым он может

посвящать свободное время.

Риск пятый - неконтролируемые покупки. Не смотря на то, что

покупки через Интернет пока еще являются экзотикой для большинства из

нас, однако недалек тот час, когда эта угроза может стать весьма актуальной.

Необходимо объяснить ребенку, что любые покупки, совершаемые в

Интернете или по мобильному телефону, должны осуществляться взрослым,

либо осуществляться с его разрешения. Всегда совместно принимайте

решение о том, стоит ли воспользоваться теми или иными услугами,

предлагаемыми в интернете.

9

Кроме того, по незнанию, неопытности, под воздействием рекламы

ребенок может совершить покупки с помощью счета сотовой связи, поэтому

в сотрудничестве с оператором установите необходимые блокировки для

телефона, сообщений SMS или ограничения расходов в мобильном телефоне

ребенка.

И, конечно же, не оставляйте в свободном для ребенка доступе

банковские карты и платежные данные, воспользовавшись которыми ребенок

может самостоятельно совершать покупки.

Это поможет избежать последствий столкновения ребенка с

негативным опытом в Интернете. Положительный эмоциональный

контакт ребенка с родителями поможет расположить его к трудному

разговору о том, что произошло. Ребенок должен вам доверять и

понимать, что вы тоже обеспокоены и хотите разобраться в ситуации

и помочь ему, но ни в коем случае не наказать.

Надеюсь, сегодняшняя беседа поможет вам чувствовать себя а

безопасности на просторах интернета и помогать своим детям избегать

неприятностей в киберпространстве.

Спасибо за внимание!