УТ МВД России по СКФО

ТАГАНРОГСКИЙ ЛИНЕЙНЫЙ ОТДЕЛ МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ НА ТРАНСПОРТЕ (Таганрогский ЛО МВД России на транспорте)

пл. Восстания, д. 1, г. Таганрог,
Ростовской области, 347904
тел. /факс (8634) 687-503

14.02.2025 № 780

на № _____от_____

Начальнику Управления образования г. Таганрога

Морозовой О.Л.

г. Таганрог,
пер. Красногвардейский, д. 1
347900

о направлении информации

Уважаемая Ольга Львовна!

Сотрудниками Таганрогского ЛО МВД России на транспорте проводятся мероприятия, направленные на предупреждение кибермошенничеств с использованием информационно-телекоммуникационных технологий - сети Интернет, средств мобильной связи, расчетных пластиковых карт, подменной телефонии.

В современных реалиях дроперами[1] становятся все чаще несовершеннолетние. Мошенники зачастую используют несовершеннолетних, которые передают персональные данные родителей и близких родственников, данные банковских карт. Продают такую информацию для получения «легких денег», тем самым становятся соучастниками преступлений. Защитить подростков можно за счет повышения финансовой грамотности, как детей, так и и родителей.

В целях профилактики кибермошенничеств просим Вас оказать содействие по размещению информационного материала разъясняющих правила безопасного поведения в сети «Интернет», поступившего из УТ МВД России по СКФО, на официальных сайтах, муниципальных организаций общего и

[1] Дропер – это человек, который сознательно или случайно предоставляет свои банковские реквизиты мошенникам для проведения незаконных операций.

дошкольного образования г. Таганрога, а также на сайте Управления образования г. Таганрога.

О принятых мерах прошу Вас сообщить в адрес Таганрогского ЛО МВД России на транспорте в срок до 22.02.2025.

Начальник ОПДН О.М. Мертешова

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 148320F7F9BD2DEA68ACC10F273ED351
Владелец **Мертешова Ольга Михайловна**
Действителен с 13.01.2025 по 08.04.2026

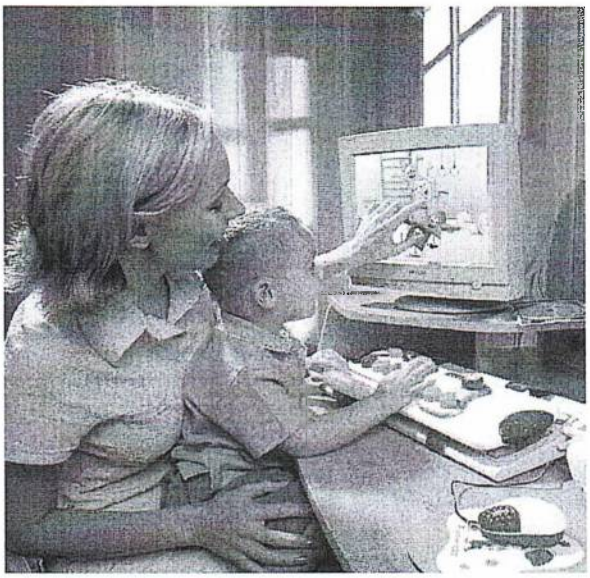
исп.: И.Ю. Иваненко
тел.: 687-531

СЭД МВД
№1-1534 от 12.02.2025

ПАМЯТКА ДЛЯ РОДИТЕЛЕЙ «БЕЗОПАСНОСТЬ ДЕТЕЙ В ИНТЕРНЕТЕ: ВОЗРАСТ И ЭТАПЫ РАЗВИТИЯ»

В нашем современном мире пользователи Сети становятся все моложе. Благодаря Интернету дети открывают для себя новый мир, получают огромное количество информации, знакомятся и общаются, занимаются творчеством.

Безопасность в Интернете детей от 2 до 5 лет



В этом возрасте дети уделяют собственно Интернету мало внимания. Однако онлайновые изображения и звуки могут стимулировать воображение и развивать фантазию ребенка.

ЧТО РЕБЕНОК МОЖЕТ ДЕЛАТЬ В ИНТЕРНЕТЕ:

Родители, а также старшие братья и сестры, могут выходить в Интернет вместе с дошкольниками для посещения детских сайтов и игр, общения по скайпу с родными и близкими.

Советы по безопасности

- Дети этого возраста должны выходить в Интернет только под присмотром родителей.
- Добавьте сайты, которые вы часто посещаете, в список Избранное, чтобы создать для детей личную интернет-среду.
- Используйте рассчитанные на детей поисковые машины (наподобие MSN Kids Search) или поисковые машины с фильтрами информации.
- Используйте средства блокирования нежелательного материала (напри-мер, MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- Помогите защитить детей от назойливых всплывающих окон с помощью специальных программ. Это функция также встроена в Windows XP с последним обновлением и в панель инструментов MSN.
- Когда маленькие дети начинают осваивать Сеть, остальные члены семьи должны служить для них примером.

Безопасность в Интернете детей от 5 до 7 лет

У детей этого возраста обычно открытая натура и положительный взгляд на мир.

Они доверяют авторитету взрослых, хотят вести себя хорошо, гордятся приобретенным умением читать и считать, готовы к новым познаниям и творчеству.

ЧТО РЕБЕНОК МОЖЕТ ДЕЛАТЬ В ИНТЕРНЕТЕ:

Играть, готовиться к школе, участвовать в конкурсах, общаться.

Однако дети этого возраста сильно зависят от взрослых при поиске сайтов, интерпретации информации из Интернета или отправке электронной почты.

Советы по безопасности

- Добавьте сайты, которые вы часто посещаете, в список Избранное, чтобы создать для детей личную интернет-среду.
- Используйте рассчитанные на детей поисковые машины (наподобие MSN Kids Search) или поисковые машины с фильтрами информации.
- Используйте средства блокирования нежелательного материала (напри-мер, MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.

- Помогите защитить детей от назойливых всплывающих окон с помощью специальных программ. Это функция также встроена в Windows XP с последним обновлением и в панель инструментов MSN.
- Расскажите детям о конфиденциальности. Научите их никогда не выдавать в Интернете информацию о себе и своей семье. Если на сайте необходимо, чтобы ребенок ввел имя, помогите ему придумать псевдоним, не раскрывающий никакой личной информации, объясните, для чего это нужно.
- Не разрешайте детям этого возраста пользоваться службами мгновенного обмена сообщениями, чатами или досками объявлений, самостоятельно отправлять письма по электронной почте.
- Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повторится. Получите дополнительную информацию об обращении с интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы

Безопасность в Интернете детей от 7 до 9 лет

Детей этой возрастной группы (как правило, ученики 1-3 классов) только начинают развивать чувство своей моральной и половой индивидуальности.

Они доверчивы и не сомневаются в авторитетах, часто интересуются жизнью старших детей.

Однако в этом возрасте у детей появляется желание выяснить границы свободы: что они могут себе позволить делать без разреше-ния родителей.

ЧТО РЕБЕНОК МОЖЕТ ДЕЛАТЬ В ИНТЕРНЕТЕ:

Дети этого возраста любят путешествовать по Интернету и играть в сетевые игры. Возможно, они используют электронную почту и могут также заходить на сайты и чаты, посещать которые родители не разрешали.

Советы по безопасности

- Создайте список домашних правил Интернета при участии детей.
- Приучите детей посещать строго те сайты, которые вы разрешили.
- Держите компьютеры с подключением к Интернету в общих комнатах.
- Используйте рассчитанные на детей поисковые машины (наподобие MSN Kids Search) или поисковые машины с фильтрами информации.
- Используйте средства блокирования нежелательного материала (напри-мер, MSN Premium's Parental Controls) как дополнение (не замену) к родитель-скому контролю.

- Создайте семейный электронный ящик вместо того, чтобы позволять детям иметь собственные адреса.
- Научите детей советоваться с вами перед раскрытием информации через электронную почту, чаты, доски объявлений, регистрационные формы и личные профили.
- Научите детей не загружать программы, музыку или файлы без вашего разрешения.
- Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или содержащих определенные слова или фразы.
- Не разрешайте детям этого возраста пользоваться службами мгновенного обмена со-общениями.
- Позволяйте детям заходить на детские сайты только с хорошей репутацией и контролируемым общением.
- Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
- Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между полами, так как в Интернете дети могут легко натолкнуться на порнографию или сайты «для взрослых».
- Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит или угрожает им. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам. Похвалите их и побуждайте подойти еще раз, если случай повто-

рится. Получите дополнительную информацию об обращении с интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы

Безопасность в Интернете детей от 9 до 13 лет

Этот возраст – время быстрых изменений в жизни.

Хотя дети все еще сильно зависят от своих родителей, они уже хотят некоторой свободы. Ребята начинают интересоваться окружающим миром, и отношения с друзьями становятся для них по-настоящему важными.

ЧТО РЕБЕНОК ДЕЛАЕТ В ИНТЕРНЕТЕ:

Дети этого возраста используют интернет для разработки школьных проектов. Кроме того, они загружают музыку, пользуются электронной почтой, играют в игры онлайн, заходят на фанатские сайты своих кумиров. Их любимый способ общения – мгновенный обмен сообщениями.

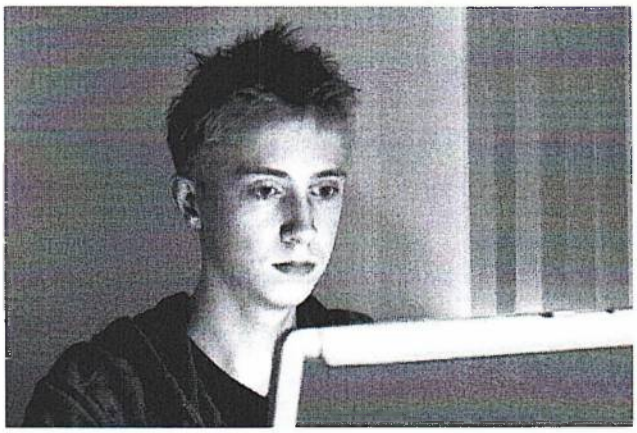
Советы по безопасности

- Создайте список домашних правил Интернета при участии детей.
- Держите компьютеры с подключением к Сети в общих комнатах, а не в спальнях детей.
- Используйте средства фильтрования нежелательного материала (наподобие MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются так, как если бы речь шла о друзьях в реальной жизни.
- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
- Позволяйте детям заходить на детские сайты только с хорошей репутацией и контролируемым общением.
- Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Познакомьте их с информационно-развлекательный сайтом, для детей и подростков открытом Роскомнадзором http://персональныеданные.дети/.
- Научите детей не загружать программы без вашего разрешения – они мо-гут ненарочно загрузить вирус или шпионскую программу. Кроме того, объясните ребятам, что, делая файлы общими или загружая из Интернета тексты, фотографии или рисунки, они могут нарушать чьи-то авторские права.
- Чтобы ребенок не мог заниматься чем -то посторонним без вашего ведома, создай-те ему учетную запись с ограниченными правами.
- Приучите детей сообщать вам, если что-либо или кто- либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай по-

вторится. Получите дополнительную информацию об обращении с интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы *(подробнее: на стр. 9)*.

- Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между полами, так как в Интернете дети могут легко натолкнуться на порнографию или сайты «для взрослых».
- По-прежнему пользуйтесь семейным электронным ящиком вместо того, чтобы позволять детям иметь собственные адреса, либо настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами.
- Расскажите детям об ответственном, достойном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

Безопасность в Интернете детей от 13 до 17 лет



Младшие подростки, как правило, проходят через период низкой самооценки; ищут поддержку у друзей и неохотно слушают родителей.

Те, кто постарше – ищут свое место в мире и пытаются обрести собственную независимость. В этом возрасте подростки уже полноценно общаются с окружающим миром. Они бурлят новыми мыслями и идеями, но испытывают недостаток жизненного опыта.

Родителям важно продолжать следить, как в этом возрасте их дети используют Интернет.

ЧТО ПОДРОСТКИ ДЕЛАЕТ В ИНТЕРНЕТЕ:

Они скачивают музыку, пользуются электронной почтой, службами мгновенного обмена сообщениями и играют. Большинство пользуются чатами, общаются в приватном режиме.

Мальчики в этом возрасте склонны сметать все ограничения и жаждут грубого юмора, крови, азартных игр и картинок для взрослых.

Девочкам больше нравится общаться в чатах; и юные дамы более чувствительны к сексуальным домогательствам в Интернете.

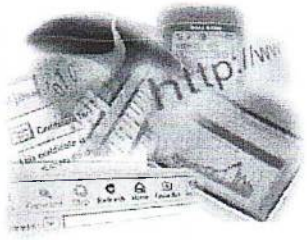
В данном возрасте родителям часто уже весьма сложно контролировать своих детей, так как об Интернет они уже знают значительно больше своих родителей.

Тем не менее, особенно важно строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернет. Следует обратить внимание на необходимость содержания родительских паролей (паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности

- Создайте список домашних правил Интернета при участии подростков. Следует указать список запрещенных сайтов, часы нахождения в Сети и руководство по общению в Интернете (в том числе и в чатах).
- Держите компьютеры с подключением к Интернету в общих комнатах.
- Беседуйте с детьми об их друзьях в Интернете и о том, чем они занимаются, так, как если бы речь шла о друзьях в реальной жизни. Спрашивайте о людях, с которыми подростки общаются, используя мгновенный обмен сообщениями, и убедитесь, что эти люди им знакомы.
- Используйте средства блокирования нежелательного материала (например, MSN Premium's Parental Controls) как дополнение (не замену) к родительскому контролю.
- Знайте, какими чатами и досками объявлений пользуются дети и с кем они общаются. Поощряйте использование модерируемых чатов и настаивайте, чтобы подростки не общались с кем-то в приватном режиме.
- Настаивайте, чтобы они никогда не соглашались на личные встречи с друзьями из Интернета без вашего сопровождения на первой встрече (или сопровождения дру-гого взрослого, которому вы доверяете). Объясните, что если виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к заботе подростка о собственной безопасности.
- Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в Интернете. Познакомьте их с информационно-развлекательный сайтом, для детей и подростков открытом Роскомнадзором http://персональныеданные.дети/.
- Научите детей не загружать программы, музыку или файлы без вашего разрешения . Объясните, что иначе подростки могут нарушить авторские права и тем самым закон.
- Приучите детей сообщать вам, если что-либо или кто-либо в Сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай повторится. Получите дополнительную информацию об обращении с интернет-преступниками и интернет-преступниками и хулиганами. Сообщите о негативном контенте в компетентные органы *(подробнее: на стр. 9).*
- Говорите с детьми о традиционных семейных ценностях, взаимоотношениях между полами, расскажите детям о порнографии в интернете и противоправности ее распространения, направьте их на хорошие сайты о здоровье, вреде ранних половых контактов, предупреждении подростковой беременности.
- Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
- Возьмите за правило знакомиться с сайтами, которые посещают подростки. Убедитесь, что дети не посещают сайты с оскорбительным содержимым, не публикуют личную информацию или свои фотографии.
- Напоминайте детям об ответственном, достойном поведении в Интернете. Ребята ни в коем случае не должны использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- Убедитесь, что подростки советуются с вами перед покупкой или продажей чего-либо в Интернете.
- Обсудите с подростками азартные сетевые игры и их возможный риск. Напомните, что для детей это незаконно.

Зачастую наши дети более «продвинутые» интернет-пользователи, чем мы, их родители. Обсуждать с детьми их путешествия в Сети поможет приведенная ниже информация.



Список терминов

- **Аккаунт** (англ.- account) – учетная запись, регистрационная запись.
- **Антивирус** – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной систе-мы вредоносным кодом.
- **Администраторы, модераторы сайта** – специальные сотрудники сайта, которые следят за исполнением установленных на сайте правил.
- **Базы данных (БД)** – специальное программное обеспечение, предназначенное для организации хранения и доступа к данным (информации). Используются при создании программных решений для автоматизации сайта.
- **Браузер** – программа, позволяющая просматривать страницы в сети Интернет. Самые популярные Opera, Mozilla Firefox, Google Chrome, Internet Explorer.
- **Веб-сайт** (англ. Website, от web – паутина и site – «место») в компьютерной сети. Когда говорят «своя страничка в Интернет», то подразумевается целый веб-сайт или личная страница в составе чужого сайта. Кроме веб-сайтов в сети Интернет так же доступны WAP-сайты для мобильных телефонов.
- **Виртуальный собеседник** (англ. chatterbot) – это компьютерная программа, которая создана для имитации речевого поведения человека при общении с одним или несколькими пользователями.
- **Всемирная паутина** – это все веб-сайты Интернета.
- **Домен** (англ. domain), Доменный адрес (англ. domain name) – область пространства иерархических имен сети Интернет, которая обозначается уникальным именем. Это более практичный аналог IP-адреса, обозначаемого цифрами. Доменная адресация возникла в Интернет для удобства пользователей: легче запомнить доменный адрес (например, www.microsoft.com), чем числа IP-адреса. Доменный адрес может содержать латинские буквы, цифры, точки и некоторые другие знаки.
- **Доменный почтовый ящик**, в который поступает почта, приходящая на любые возможные адреса домена (все-что-угодно@ваш-домен).
- **Интернет**– всемирная система объединённых компьютерных сетей для хранения и передачи информации.
- **Игнор** – игнорирование, занесение в черный список.
- **Кибербуллинг** – травля через Интернет, электронную почту, СМС и т. д., агрессивное преследование одного из членов коллектива (школьников или студентов) со стороны остальных членов коллектива или его части.
- **Логин** (от английского log in — «входить в») – это имя, которое вы выбираете для регистрации в системе или имя, которое система вам сама присваивает. Каждый пользователь в системе имеет свой уникальный логин. Он помогает системе и другим пользователям отличить одного пользователя от другого.
- **Он-лайн игры** – игровой процесс основан на взаимодействии с другими игроками и игровым миром, требующий постоянного подключения к Интернету.
- **Интернет-магазин**. Действующим Законодательством РФ не определено понятие «Интернет-магазин». В классическом понимании "Интернет-магазин" ("Электронный магазин", "Сетевой магазин"; и т.д.), – это интерактивный сайт, в котором: рекламируются

товары и услуги, принимаются заказы на товары и услуги, посетителю, предлагаются различные варианта оплаты заказанных товаров и услуг, возможна их мгновенная оплата через Интернет.

- **Пароль** – набор символов, известный только одному пользователю, необходимый для авторизации (для «входа») на сайте.
- **Персональная страница** (персональный сайт) – совокупность Web-страниц, с содержанием, описывающим сферу интересов какого-либо человека (группы лиц), обычно созданная им самим.
- **Посетители** – количество уникальных посетителей побывавших на страницах вашего ресурса.
- **Почтовый ящик** - дисковое пространство на почтовом сервере, выделенное для хранения, отправки писем пользователя и т.д. (приходящих на его адрес и подлежащих отправке).
- **Родительский контроль** – это программы и службы, которые позволяют родителям и опекунам отслеживать, как ребенок использует компьютер: от фильтрации веб-содержимого и управления контактами электронной почты до ограничений на общение через Интернет. Цель таких средств — обеспечить безопасность ребенка в Интернете, и эти инструменты иногда называют семейными настройками и настройками семейной безопасности. Windows 7, Windows Vista, Xbox 360, Xbox Live, Bing и другие продукты Microsoft включают встроенные настройки семейной безопасности.
- **Сайт** (от англ. website: web — «паутина, сеть» и site — «место», буквально «место, сегмент, часть в сети») – совокупность электронных документов (файлов) частного лица или организации в компьютерной сети, объединённых под одним адресом (доменным именем или IP-адресом).
- **Сервер** (Web-сервер) -1) Компьютер или специализированное устройство в сети со специальным программным обеспечением, обеспечивающий доступ многих пользователей к расположенной на нем информации и функционирование любых необходимых сервисов Интернет: http (сайт), E-mail (электронная почта), конференции, ftp и т.п. Для размещения сайта в Интернет необходим веб-сервер с поддержкой как минимум сервиса http. 2) Сайт, крупный информационный ресурс Интернета.
- **Спам** (англ. spam) – рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать, незапрошенные или нежелательные письма.
- **Социальные сети** – сайты в Интернете, на которых рядовые пользователи заводят свои странички для общения с друзьями. Одна из обычных черт социальных сетей – система «друзей» и «групп». Самые популярные русскоязычные: ВКонтакте, Одноклассники.ш, Мой Мир, Мой Круг, ЖЖ и др.
- **Трафик** (traffic) – поток (объем) информации, проходящей через канал связи, приходящийся на сайт. Может быть исходящим и входящим.
- **Тролли, троллинг** – (от англ. trolling — «ловля на блесну») – размещение в Интернете провокационных сообщений с целью вызвать конфликты между субъектами, взаимные оскорбления и т. п.
- **Файлы, скачивание**. Вся информация в компьютере сохраняется в виде файлов. Это могут быть текстовые файлы, музыкальные, видео, графические, мультимедийные и проч. Файлы можно создавать, копировать, пересылать (например, по электронной почте), выкладывать на сайт для скачивания, скачивать, то есть сохранять на свой компьютер.
- **Фишинг** (от английского fish — «ловить рыбу») – вид мошенничества в интернете, когда у пользователя пытаются узнать логины и пароли.
- «Черный список сайтов» (black list), или как еще его называют "скам лист", представляет собой список сайтов, проектов или людей, которые проводят мошеннические операции в сети или не выполняют взятые на себя обязательства.

- **Хиты** – количество просмотров страниц, на которых побывали посетители ресурса.
- **Хостер** (hoster) - синоним слова хостинг-провайдер (см.)
- **Хостинг** (hosting) - Услуга по предоставлению интернет-сервера и обеспечению его круглосуточной работоспособности. В большинстве случаев предоставляется виртуальный сервер (т.н. виртуальный хостинг), т.е. программное обеспечение, обеспечивающее работу необходимых Вам сервисов, но работающее на одной аппаратной платформе с другими подобными виртуальными серверами. Различают также платный (коммерческий) и бесплатный хостинг.
- **Хостинг-провайдер** (hosting provider) - организация, профессионально занимающаяся предоставлением услуг Хостинга. Лучше выбирать услуги профессиональных Хостеров, т.е. Компаний, основной деятельностью которых является Хостинг, а не обычных Интернет-провайдеров, для которых Хостинг дополнительная услуга к основной.
- **Хосты** – количество посетителей с уникальным IP-адресом.
- **Электронная почта** (англ. email, e-mail, от англ. electronic mail) – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемых «письма» или «электронные письма») по распределённой (в том числе глобальной) компьютерной сети. Электронная почта по составу элементов и принципу работы практически повторяет систему обычной (бумажной) почты, заимствуя как термины (почта, письмо, вложение, ящик, доставка и другие), так и характерные особенности – простоту использования, задержки передачи сообщений, достаточную надёжность и в то же время отсутствие гарантии доставки.

СЭД МВД
№1-534 от 12.02.2025

Что включают в себя персональные данные?

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

фамилия, имя и отчество, дата и место рождения, адрес, семейное положение, паспортные данные, номер телефона, профессия, доходы, ИНН,

Нормативно-правовая база по защите персональных данных:

Где существует наибольший риск потери персональных данных ?

Социальные сети и мессенджеры

Аккаунт Google или Apple ID

Электронная почта

Банковские данные

Аккаунты в игровых сервисах

Незащищённая Wi-Fi-точка

Мобильные приложения

ЧТО ДЕЛАТЬ, ЕСЛИ ВЫ ОБНАРУЖИЛИ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ В ИНТЕРНЕТЕ?

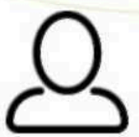
Написать жалобу →

Владелец аккаунта

Тех.поддержка

Администрация сайта

Когда невозможно установить источник распространения персональных данных или связаться с ним? напрямую ?



Нужно обратится в **Прокурату** или Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (**Роскомнадзор**).

ТОП-5 ОСНОВНЫХ СПОСОБОВ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1

Используйте двухфакторную аутентификацию

2

Контролируйте доступ приложений к вашим данным

3

Пользуйтесь менеджерами паролей

4

Используйте только защищённое соединение

5

Пользуйтесь VPN, работая с публичными Wi-Fi-точками

ЧЕМ ГРОЗИТ УТЕЧКА ПЕРСОНАЛЬНЫХ ДАННЫХ?

Завладев персональными данными, мошенники могут:

- *оформить кредит в банке;*
- *«повесить» долги или фирму;*
- *совершить незаконные действия с вашей недвижимостью;*
- *распорядиться средствами с банковских карт;*
- *открыть электронный кошелек;*
- *зарегистрироваться на сайтах знакомств, онлайн-игр и казино;*
- *шантажировать вас или ваших родственников;*
- *использовать вашу личность как «подменную» для мошеннических действий;*
- *устроить кибербуллинг;*
- *использовать ваши данные в собственных интересах, например, навязывать услуги, распространять противоправный контент.*

Поговорим о цифрах

47% россиян зарегистрированы в социальных сетях;

6,5 часов в сутки — средняя продолжительность времяпрепровождения в сети «Интернет»;

46% наших соотечественников постоянно совершают онлайн-покупки.

Отчет «Global Digital 2018», подготовленный аналитическим агентством «We Are Social» и SMM-платформой «Hootsuite

Больше полезной информации: http://персональныеданные.дети/

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА ЗЛОУМЫШЛЕННИКОВ В СЕТИ ИНТЕРНЕТ

Авторы :
Алиев А.М, Жученко В.С, Саенко Д.А.

СЭД МВД
№1-1534 от 12.02.2025

Интернет – это безграничный мир информации. Здесь ты найдёшь много интересного и полезного для учёбы. В интернете можно общаться со знакомыми и даже заводить друзей.

Но кроме хорошего, в виртуальном мире есть и плохое. Неправильное поведение в интернете может принести вред не только тебе, но также твоим родным и близким.

Чтобы обезопасить себя в интернете, достаточно соблюдать правила, которые содержатся в этой памятке. В этих правилах нет ничего трудного. Отнесись к ним внимательно – и расскажи о них своим друзьям!

Тест на знание правил поведения в интернете

1) Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.
   - А Попрошу его фото, и потом отправлю своё.
   - В Посоветуюсь с родителями.
2) В чате тебя обозвали очень грубыми словами.
   - А Скажу в ответ: «Сам дурак».
   - В Прекращу разговор с этим человеком.
3) Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.
   - А Потребую доказательств, что она плохая.
   - В Сразу откажусь.
4) Пришло сообщение с заголовком «От провайдера» – запрашивают твой логин и пароль для входа в Интернет.
   - А Вышлю только пароль: они сами должны знать логин.
   - В Отмечу письмо как Спам.

Посчитай, сколько получилось ответов «А» и сколько «В».

4 «А»
Тебе ещё многому надо научиться.

3 «А» и 1 «В»
Внимательно прочитай эту памятку.

2 «А» и 2 «В»
Неплохо, но ты защищён лишь наполовину.

1 «А» и 3 «В»
Ты почти справился, но есть слабые места.

4 «В»
Молодец! К Интернету готов!

Министерство внутренних дел Российской Федерации

Управление «К»

Безопасный интернет – детям!

Полезные советы для тебя и твоих друзей

ОСТОРОЖНО:

ВИРУСЫ И ДРУГИЕ ВРЕДОНОСНЫЕ ПРОГРАММЫ (ЧЕРВИ, ТРОЯНЫ)

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья.

Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут **уничтожить** важную информацию **или украсть** деньги через Интернет.

- **Для защиты компьютера** на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
- **Не сохраняй подозрительные файлы** и не открывай их.
- Если антивирусная защита компьютера не рекомендует, **не заходи на сайт, который считается «подозрительным».**
- Никому **не сообщай свой логин с паролем** и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.

ВИРТУАЛЬНЫЕ МОШЕННИКИ (ВОРЫ) И ДРУГИЕ ПРЕСТУПНИКИ ИНТЕРНЕТА

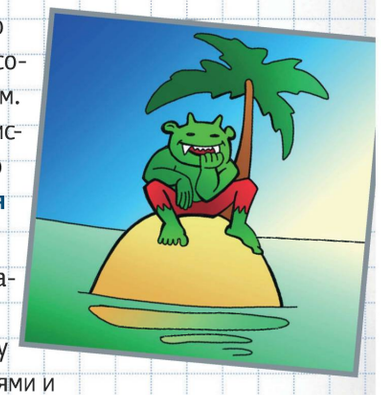
Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- **Не сообщай свой адрес или телефон** незнакомым людям и никогда не выкладывай в Интернете. Никогда **не высылай свои фотографии** без родительского разрешения. Помни, что **преступники могут использовать эту информацию** против тебя или твоих родных.
- **Если ты хочешь поучаствовать** в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
- Никогда **не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете.** Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника **может скрываться взрослый человек с преступными намерениями.**

ГРУБИЯНЫ И ХУЛИГАНЫ (ТРОЛЛЬ, ПРОВОКАТОР) В ИНТЕРНЕТЕ: КАК СЕБЯ ВЕСТИ?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

- Помни: **ты не виноват**, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекрати общение.
- **Если тебе угрожают** по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз – испугать тебя и обидеть. Но **подобные люди боятся ответственности.**



- Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. **Никогда не участвуй в травле и не общайся с людьми, которые обижают других.**
- Всегда **советуйся с родителями** во всех указанных случаях.

СЭД МВД
№1-1534 от 12.02.2025

КАКИЕ УГРОЗЫ СУЩЕСТВУЮТ В СЕТИ ИНТЕРНЕТ?

КИБЕРБУЛЛИНГ

Интернет - мошенничество

ПРОПАГАНДА НАРКОТИКОВ И АЛКОГОЛЯ

ИГРОМАНИЯ

ЧТО ДЕЛАТЬ РОДИТЕЛЯМ?

Не пытайтесь насильно ограничивать ребенка в использовании сети Интернет

Частая ошибка родителей: мы пытаемся сократить время пребывания ребенка в сети, вместо того, чтобы работать над качеством. Ребенок может провести час на сайте с опасным контентом и два часа на образовательном канале. Работайте НЕ над временем.

Будьте друзьями

В 13-17 лет нужно быть максимально лояльными с детьми, вряд ли они будут доверять тирану.

Не забывайте беседовать с детьми об их друзьях в интернете, о том, чем они заняты, таким образом, будто речь идет о друзьях в реальной жизни. Делайте беседу непринужденной. Помните, допросы только оттолкнут.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом

Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

ЧТО ДЕЛАТЬ РОДИТЕЛЯМ?

Приучите себя знакомиться с сайтами, которые посещают подростки

Делайте это аккуратно, чтобы у ребенка не возникало чувство излишнего контроля над ним. Регистрируйтесь во ВКонтакте, Instagram, обычно именно там подростки делятся своими новостями и мыслями.

Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям. Напомните, что это противоречит не только морали, но и закону.

Обсудите с ребенком его новости в социальных сетях. Предупредите о том, что любая фотография, текст навсегда остаются в интернете, независимо от того, удалили ее с личной страницы или нет. Прежде чем что-то публиковать - пусть ребенок подумает: не отразится ли это на его будущем?

СЭД МВД
№1-1534 от 12.02.2025

НЕ ПОНИМАЕТЕ О ЧЕМ ГОВОРИТ ВАШ РЕБЕНОК?

Кринж - это отвращение, например отвратительные бессмысленные ролики вызывают много кринжа.

Краш - человек, который нравится.

Изи используется в играх и иногда в жизни, что-то легкое и простое, даже слишком!

Хайповый означает модный, в теме, шарит что происходит в мире моды. **Хайп** это то, что сейчас модно. **Хайпим** означает тусим, развлекаемся, зажигаем.

Трэш - вещь, которая уже не актуальна. **Трэшиться** - то есть прикалываться, делать что-то не всерьёз.

Шер - поделиться чем-то в социальной сети.

КОНТАКТЫ

НЦПТИ

ИНТЕРНЕТ БЕЗ УГРОЗ

Национальный центр информационного противодействия терроризму и экстремизму в образовательной среде и сети Интернет

Веб-сайт: НЦПТИ.РФ
Телефон: (863) 201-28-22
E-mail: info@ncpti.ru

Министерство общего и профессионального образования Ростовской области

Веб-сайт: http://www.rostobr.ru
Телефон: (863) 240-34-97
E-mail: min@rostobr.ru

Безопасность детей в интернете

КАКИЕ УГРОЗЫ СУЩЕСТВУЮТ В СЕТИ ИНТЕРНЕТ?

КИБЕРБУЛЛИНГ

Интернет - мошенничество

ПРОПАГАНДА НАРКОТИКОВ И АЛКОГОЛЯ

ИГРОМАНИЯ

ЧТО ДЕЛАТЬ РОДИТЕЛЯМ?

Не пытайтесь насильно ограничивать ребенка в использовании сети Интернет

Частая ошибка родителей: мы пытаемся сократить время пребывания ребенка в сети, вместо того, чтобы работать над качеством. Ребенок может провести час на сайте с опасным контентом и два часа на образовательном канале. Работайте НЕ над временем.

Будьте друзьями

В 13-17 лет нужно быть максимально лояльными с детьми, вряд ли они будут доверять тирану.

Не забывайте беседовать с детьми об их друзьях в интернете, о том, чем они заняты, таким образом, будто речь идет о друзьях в реальной жизни. Делайте беседу непринужденной. Помните, допросы только оттолкнут.

Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с интернетом

Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

ЧТО ДЕЛАТЬ РОДИТЕЛЯМ?

Приучите себя знакомиться с сайтами, которые посещают подростки

Делайте это аккуратно, чтобы у ребенка не возникало чувство излишнего контроля над ним. Регистрируйтесь во ВКонтакте, Instagram, обычно именно там подростки делятся своими новостями и мыслями.

Объясните детям, что ни в коем случае нельзя использовать сеть для хулиганства, распространения сплетен или угроз другим людям. Напомните, что это противоречит не только морали, но и закону.

Обсудите с ребенком его новости в социальных сетях. Предупредите о том, что любая фотография, текст навсегда остаются в интернете, независимо от того, удалили ее с личной страницы или нет. Прежде чем что-то публиковать - пусть ребенок подумает: не отразится ли это на его будущем?