АЗБУКА ИНТЕРНЕТ-БЕЗОПАСНОСТИ

ДЛЯ РОДИТЕЛЕЙ

ЦЕНТР БЕЗОПАСНОГО ИНТЕРНЕТА

НЕ ДОПУСТИ!

РОЦИТ

ОБЩЕСТВЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ
CIVIC CHAMBER OF THE RUSSIAN FEDERATION

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE

ins@fe

Наверное, излишне говорить, что наш повседневный мир давно стал «цифровым» - буквально пронизанным цифровыми технологиями. Пожалуй, впервые в своей истории человек получил возможность делать кучу важных для своей жизни вещей, не выходя из дома – такой возможности не предоставлял даже появившийся сто с лишним лет назад телефон. И уж тем более телефон не породил такое обилие сервисов, дающих нам новые возможности, не представимые еще три десятилетия назад.

Интернет-мир породил свою лексику, сленг и даже собственную субкультуру, которой «цифровые аборигены» - те, кто впитал цифровые технологии буквально с молоком матери – активно пользуются. Казалось, что онлайн-возможности породят даже собственную этику, в корне отличную от привычной нам. Это, конечно же, не так – отдельной «этики виртуального мира» не существует, как не существует и самого отдельного «виртуального мира». Однако своя терминология и своя субкультура применительно к процессам в Сети все же существует и является данностью. Некоторые слова, привычные нам по «доинтернетной» эпохе, поменяли смысл и применительно к Интернет-отношениям могут значить нечто совершенно специальное. А иногда смысл остается схожим, но «что конкретно там имели в виду», неосведомленный человек все-таки до конца не представляет. Знание этого «Интернет-языка» зачастую критично для обеспечения «цифровой безопасности» - как безопасности детей, так и взрослых.

В нашей «Азбуке» раскрываются некоторые термины, понятия и элементы сленга, регулярно циркулирующие в Интернете и используемые для описания Интернет-процессов. Некоторые из них используются только молодежью или, скажем, игроками онлайн-игр, некоторые – специалистами. Часть слов, раскрываемых в нашей «Азбуке», служит для описания угроз, представляющих серьезную опасность в онлайне. Однако это не просто «толковый словарь» - это справочник по безопасности, и все приводимые в «Азбуке» понятия рассматриваются именно с точки зрения обеспечения «цифровой безопасности». Поэтому применительно к каждой «статье» нашей «мини-энциклопедии» Вы найдете краткие правила безопасности в Сети, связанные с этим понятием или термином.

Надеемся, что с нашей «Азбукой» Вам станет немного легче разговаривать с Вашими «интернетизированными» детьми на одном языке и помочь им защититься от тех опасностей, которые так или иначе порождает «цифровой мир».

Центр безопасного Интернета в России

Центр детской безопасности в информационном обществе «НеДопусти!»

А

АВАТА́Р (он же ава́та́ра, он же ава́та́рка, он же а́ва, он же юзерпи́к – от английского user picture — картинка пользователя) — это фотография или картинка, представляющая пользователя в виртуальных просторах. Проще говоря, это «лицо» пользователя в Сети. Аватары используются на форумах, в чатах, блогах, социальных сетях, различных играх.

В оффлайне происхождение этого термина обычно ищут в философии индуизма. На русский язык «аватар» обычно переводится как «воплощение» - кого-либо в ином образе. Именно поэтому термин «аватар» прижился применительно к изображению, олицетворяющему пользователя Интернет-сервиса.

Аватаром может быть реальная фотография человека или любая другая картинка – хотя, строго говоря, под аватаром понимают изображение какого-либо персонажа (некоторые пользователи ставят в качестве юзерпика, к примеру, какой-нибудь пейзаж). Соответственно, в качестве аватара может выступать реальная фотография пользователя, по которой его можно идентифицировать, фото пользователя в более раннем возрасте, фотография другого человека (в том числе персонажа из фильма), рисованное изображение (в том числе персонаж из комикса или мультфильма) или даже карикатура. Пользователь имеет возможность периодически менять картинку-аватар.

Аватар – часть «виртуального Я» Интернет-юзера. Еще один его элемент - никнейм (он же «ник»), то есть прозвище, которым пользователь называет себя в Сети. Он тоже может быть выдуманным или реальным именем – однако, в отличие от аватара, ники крайне редко включают в себя полные фамилию, имя и отчество реального пользователя.

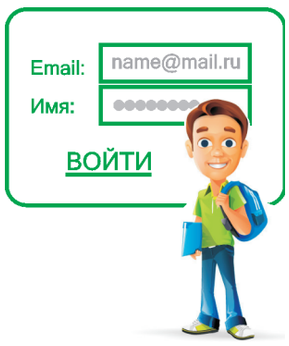
ПРАВИЛА БЕЗОПАСНОСТИ В первую очередь мнение о пользователе складывается именно по его аватару. Поэтому при выборе аватара следует быть весьма осторожным и разборчивым. Как говорится в известной пословице, «Встречают по одежке, а провожают по уму».

Аватар – обязательная часть «ложной идентичности» пользователя в Интернете, к которой часто прибегают злоумышленники. К примеру, педофил, желающий выдать себя за ребенка, нередко выбирает для аватара именно детскую фотографию – первым впечатлением его собеседника становится то, что он беседует именно с ребенком. Поэтому всегда следует помнить о том, что аватар далеко не всегда говорит о том, с кем реально мы беседуем в Сети.

Впрочем, проблема поиска «популярности» в Интернете породила и обратную проблему – нередко пользователи ставят в аватар собственную фотографию, которая призвана «произвести впечатление» на собеседников. Нередко это фотографии так называемого «секстинга», то есть собственные откровенные фото. В связи с этим ни детям и подросткам, ни взрослым настоятельно не рекомендуется ставить подобные фотографии на заставку, это может привлечь Интернет-злоумышленников и сделать Вас или Вашего ребенка жертвой Интернет-угрозы (от вовлечения в противоправную эксплуатацию до киберунижения). Подобные «шокирующие» фото, как правило, негативно воздействуют на репутацию пользователя – их могут

увидеть учителя, соседи или просто знакомые. По тем же причинам безопасности не следует ставить в аватар (и публиковать вообще) фотографии, демонстрирующие высокий уровень материального благополучия – это может привлечь вполне оффлайновых грабителей.

Не следует также ставить на аватар фотографии других реальных людей. У других пользователей создается впечатление, что действие совершается от имени человека на фото, поэтому может получиться так, что таким образом наносится ущерб репутации другого человека. Если же именно это и является целью такого шага, следует помнить, что за это предусмотрена ответственность по закону.



АККАУНТ – (от английского account – счет). Очень часто аккаунтом называют страничку в социальной сети. На самом деле аккаунт – это учетная запись для входа на сайт, в электронную почту, форум или чат. То есть «электронная узнавалка» пользователя для конкретного сайта.

Аккаунт хранит определенные данные, которые должен знать только сам пользователь. Обычно это адрес электронной почты, а так же логин и пароль (password). Аккаунт предназначен исключительно для удобства пользователя, к нему «привязана» вся Ваша деятельность на том или ином ресурсе. Данные Вашего аккаунта (также как и Ваш IP) считаются конфиденциальной информацией и не должны быть видны другим пользователям – за исключением того, что вы сами разрешите им видеть о себе. Данные, от которых зависит вход на сайт (логин и пароль), должны быть известны только Вам, а пароль вообще хранится на сервере в зашифрованном виде. Например, администратор гостевой книги может только удалить Ваш аккаунт из своей гостевой книги, но прочитать конфиденциальную информацию или установить новый пароль за вас он не может.

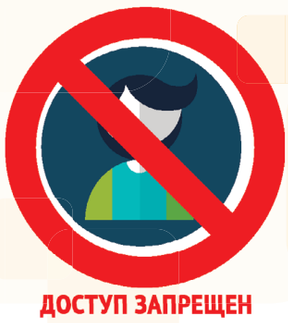
ПРАВИЛА БЕЗОПАСНОСТИ Аккаунт всегда персонален, даже если и заводится от имени организации. Данные аккаунта – это ключ к «цифровой идентичности» человека на Интернет-ресурсе, включая Интернет-банкинг. Поэтому данные своего аккаунта следует беречь примерно так же, как PIN-код к банковской карте.

Именно поэтому Интернет-мошенники активно охотятся за паролями к учетным записям (аккаунтам) пользователей. В некоторых случаях они пытаются «выманить» эти данные из доверчивых пользователей, представляясь администраторами или модераторами ресурсов. Обычно они пишут, что на сайте якобы имел место «сбой», и для восстановления работы сайта требуются пароли пользователей. Это неправда. Администратор или модератор сайта никогда не потребует у вас полные данные Вашего аккаунта - якобы для проверки его подлинности или начисления бонусов. Если кто-то просит такие данные – это мошенники. Никому не высылайте пароль от своего аккаунта!

Б

БАН (от английского ban — запрещать, объявлять вне закона) - наиболее жесткая форма наказания нарушителей правил поведения в Сети и контроля за их поведением. Обычно это означает лишение некоего пользователя возможности писать сообщения и/или отвечать на них, или вообще заходить на сайт под своим аккаунтом. В онлайн-играх бан означает отстранение игрока от

входа в игру на срок, установленный ее правилами. В зависимости от тяжести нарушения (начиная от оскорбления игроков, создания помех при игре и заканчивая мошенничеством) бан может быть на несколько дней, месяцев, а то и навсегда. Бывает и «бан по IP» - то есть запрет на вход на сайт с данного IP-адреса, так что создание нового аккаунта «забаненному» пользователю в данном случае не поможет.



Бан накладывается администратором или модератором сайта. На некоторых сайтах бан можно обжаловать у совета модераторов. В просторечии молодежь часто называет его «баня».

ПРАВИЛА БЕЗОПАСНОСТИ При регистрации на сайте, форуме и/или онлайн-игре в большинстве случаев предлагается прочесть пользовательский договор. Иногда регистрация вовсе невозможна без выбора пункта «Согласен с правилами». Внимательно ознакомьтесь с текстом договора, особенно уделив внимание части, касающейся прав и обязанностей пользователя, и всегда помните о них. Бан накладывается именно на основе этих правил, которые Вы якобы прочитали. Если Вы допускаете к некоему ресурсу ребенка, то, ознакомившись с Правилами, перескажите их основное содержание ребенку – он должен четко понимать, что можно и что нельзя на данном ресурсе.

Возможность «отлучить» от ресурса любого злостного нарушителя присутствует на любом ресурсе, где предусмотрены аккаунты пользователей. Если Вы или Ваш ребенок стали жертвой Интернет-опасности, то нелишне помнить, что теоретически во власти модератора решить проблему самостоятельно – приняв в том числе такие жесткие меры к онлайн-агрессору. На большинстве ресурсов связаться с модератором можно путем нажатия кнопки «Пожаловаться».

БАННЕР - (от английского banner — флаг, транспарант) – «интернет-плакат», встроенный в Интернет-ресурс. Баннеры могут быть статичными (то есть представлять из себя обычную картинку), а могут быть и анимированными, то есть картинка баннера может изменяться как в мультфильме. Как правило, баннеры периодически меняются. Баннер может быть и озвучен – то есть к нему может быть привязана музыка или речь.

Баннер стал основной формой интернет-рекламы, привлекающей внимание посетителей некоего сайта к другому сайту с товарами, услугами, онлайн-игрой и т.п. Как правило, нажатие мышью на баннер приводит к переходу на рекламируемый сайт.

ПРАВИЛА БЕЗОПАСНОСТИ Необходимо помнить, что при нажатии на баннер можно оказаться на сайте совершенно иного содержания, чем изначально посещенный сайт – это могут быть как фишинговые сайты мошенников, так и просто порносайты или другие сайты неприятного содержания. Часто через баннер можно «подгрузить» на свой компьютер вирус или другую вредную программу. Поэтому будьте крайне осторожны и нажимайте на рекламный блок только хорошо известной компании или сайта. Иногда бывает, что внизу страницы отображается ссылка (реальный адрес), на которую ведет баннер – внимательно смотрите, куда она ведет. Различие адреса на баннере и реального адреса, отображающегося внизу страницы, на практике является одним из главных признаков готовящегося Интернет-мошенничества.

Как правило, от переходов на другие сайты по БАННЕРам можно защититься при помощи программы «родительского контроля», устроенной по принципу «белого списка». В некоторых случаях «родительский контроль» вообще отключит баннеры, то есть сделает их показ недоступным. Конечно, от этого пострадает зрелищность страницы (отобразится пустое поле), но зато можно быть уверенным, что ребенок не увидит баннер с чем-то, чему совершенно не место на детском сайте.

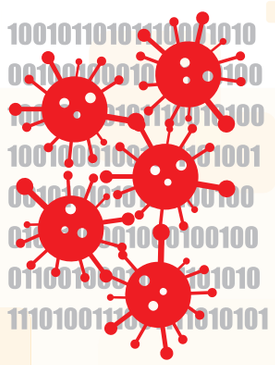
БРАУЗЕР (по-английски browser – «просматриватель») – программа, в которой открывают и смотрят веб-сайты. Практически все популярные браузеры распространяются бесплатно или «в комплекте» с операционными системами.

ПРАВИЛА БЕЗОПАСНОСТИ Безопасность компьютера – это еще и безопасность браузера. Почти все браузеры имеют собственные средства безопасности. Они могут блокировать «всплывающие окна», имеют свои фильтры от сайтов мошенников, защищают пароли. Лучше всего эти функции в браузере включать. Все эти свойства периодически обновляются, так что не будет лишним периодически обновлять свой браузер. Обновление браузеров осуществляется бесплатно.

Хакеры очень часто атакуют компьютеры, используя именно уязвимости браузеров – то есть ошибки и недоработки в их программах. Как правило, в этом случае пользователю даже не нужно скачивать и открывать какие-то файлы, достаточно просто зайти по вредоносной ссылке. Результатом такого захода, к примеру, могут быть такие сообщения в окне браузера: «Ваш компьютер инфицирован; загрузите эту антивирусную программу» - при этом под «антивирусом» на самом деле скрывается вредоносная программа.

На практике веб-антивирусы весьма успешно блокируют подобные переходы. Однако если подобное сообщение все же выскочило – следует руководствоваться «мнением» Вашего антивируса, установленного на Вашем компьютере или мобильном устройстве.

ВИРУС – вредоносная программа, созданная специально для стирания, блокирования, изменения или копирования информации на компьютере – против воли его хозяина. В разговорной речи «вирусами» привыкли называть любые вредоносные программы.



Как и любое вредоносное ПО (программное обеспечение), ВИРУСы попадают на компьютер различными способами: либо человек сам по своей доверчивости и наивности запускает на своей машине вредоносную программу, либо она запускается без участия человека, прячась в массе загружаемых программ и действуя автономно. ВИРУСы могут нарушать работу как отдельных компьютеров, так и целых компьютерных сетей. Существуют не только ВИРУСы для стационарных компьютеров, но и ВИРУСы для мобильных устройств – смартфонов и планшетов, причем популярность последних неуклонно растет с ростом аудитории мобильного Интернета.

Краткая классификация вредоносных программ выглядит следующим образом:

ЛОКАЛЬНЫЙ ВИРУС – заражает конкретный компьютер. Копия вируса попадает

на удалённые компьютеры только в том случае, если заражённый объект по не зависящим от вируса причинам оказывается на другом компьютере - например, через «флешку».

СЕТЕВЫЕ ВИРУСЫ - стандартные вирусы и «черви» (еще один вид опасных программ) могут саморазмножаться в компьютерах и компьютерных сетях, многие из них распространяются в виде файлов с расширением *exe. Однако существуют ВИРУСы, которые «живут» в форме «сетевых пакетов». «Черви» получили свое название благодаря способности проникать в компьютер без помощи пользователя. Для распространения они используют возможности локальных и глобальных сетей. Таким образом, один зараженный компьютер в скором времени способен заразить всю сеть, к которой подключен.

ТРОЯНЫ - «Троянские программы» созданы для того, чтобы пользоваться чужим компьютером, как своим – и получать с него информацию. Их название идет от «Илиады» Гомера, по аналогии с «троянским конем» - сокращением от которого и является словечко «троян». «Троян» не рушит работу компьютера, но хозяин вредоносного кода, пользуясь чужим компьютером, может украсть личную информацию жертвы, завладеть её паролями и сделать многое другое от имени законного пользователя.

Попадания на компьютер, трояны копируют себя в системные папки под «рабочими» названиями Windows. Кроме того, они прописывают себя в системном реестре, таким образом добавляясь в список программ, запускающихся при загрузке операционной системы. Сами себя копировать трояны, как правило, не умеют.

Вредоносные утилиты - разработаны для того, чтобы автоматически создавать другие вирусы, атаковать и взламывать другие компьютеры. Для «хозяйского» компьютера при этом они совершенно не опасны.

DDoS-атака – это отправка компьютеру-«жертве» многочисленных запросов через Интернет. Цель состоит в том, чтобы число запросов превысило работоспособность компьютера – в таком случае он не может с ними справиться и «зависает». Если атака производится на сервер (а так бывает чаще всего), то ввиду выхода сервера из строя становятся недоступны привязанные к нему Интернет-сайты. Зараженные вредоносной утилитой компьютеры (состоящие в бот-сети, или ботнете) участвуют в таких атаках помимо воли владельца – часто он сам даже не знает, что его компьютер кого-то атакует.

Цели злоумышленников, распространяющих вирусы:

- нажива (в таком случае их интересует денежная прибыль, кража тайной и личной информации, распространение спама, обман и вымогательство);
- нематериальная выгода (шутки, розыгрыши, хулиганство, самоутверждение).

ПРАВИЛА БЕЗОПАСНОСТИ Установите антивирус – не только на домашний компьютер и ноутбук, но и на планшет и смартфон. Дело в том, что нынешний смартфон сейчас функционально ближе к компьютеру, чем к обычному телефону. С учетом роста мобильного Интернета, увеличилось и число предложений антиви-

русов для мобильных устройств. Как правило, они производятся под все основные мобильные операционные системы (Windows Phone, Android, iOS) и при этом значительно дешевле антивирусов для «полноценных» компьютеров (на весну 2014 года их цена составляет около 300 рублей).

Регулярно следите за обновлением антивируса и скачивайте новые антивирусные базы. Что касается смартфона, то, если Ваш мобильный тариф не предусматривает безлимитного Интернета, можете обновить антивирусные базы через Wi-Fi – дома или в каком-нибудь публичном месте с устойчивым сигналом.

БУДЬТЕ ВНИМАТЕЛЬНЫ ПРИ РАБОТЕ В ИНТЕРНЕТЕ - не переходите по неизвестным ссылкам и не скачивайте подозрительные файлы.

Не верьте обещаниям «бесплатного сыра», когда вам обещают вскрыть страницу интересующего Вас пользователя или открыть еще какие-либо тайны, для чего Вам надо «лишь пройти по ссылке».

Если заражение уже произошло, есть смысл изолировать зараженный компьютер от сети.

Если Вам не удается избавиться от вредоносной программы самостоятельно – обратитесь к специалисту, но ни в коем случае не платите вымогателям (в случаях, если на экран выводится требование заплатить за «разблокировку») и не отправляйте смс-сообщения на короткие номера для такой «оплаты». Вовсе не факт, что после оплаты компьютер действительно разблокируется, а деньги Вы потеряете.

ГЕЙМЕР – (от английского gamer - игрок).

Первоначально так называли только игроков, игравших до широкого распространения Интернета в так называемые «игры по почте» (англ. play by electronic mail, игры по переписке). Эти игры были прототипами современных онлайн-игр. Классический пример - партия в шахматы, в которой соперники обменивались сообщениями о своих ходах.

Позднее словом «геймер» стали называть всех любителей компьютерных игр. Обычно их делят на тех, кто просто любит играть (казуалы), завсегдатаев-фанатов игр (хардкорщики), и профессионалов, которые даже живут на призовые деньги от игр.

ПРАВИЛА БЕЗОПАСНОСТИ Когда игра слишком сильно поглощает внимание игрока, особенно – ребенка, это может привести к тому, что виртуальный мир начнет вытеснять интерес к реальному. Стоит помнить о том, что нормальный человек всегда сумеет найти грань между миром в мониторе своего компьютера и миром за его границами. По мнению науки, продуктивным для ребенка считается времяпровождение за компьютерными играми не более одного часа в день – после чего игры начинают негативно воздействовать на память и координацию ребенка.

Кроме того, очень важно помнить, что правила поведения в обществе одинаковы везде. И от того, насколько вежливо будет вести себя игрок, зависит не только

его собственное удовольствие, но и настроение людей, окружающих его в виртуальном мире.

«ГОРЯЧАЯ ЛИНИЯ» - специальный сайт, через который можно сообщить о потенциально противоправном контенте или аналогичных действиях в Сети для того, чтобы в отношении такого контента были приняты предусмотренные законом меры. «Горячие линии» подобного рода, как правило, не принадлежат правоохранительным органам, хотя обычно работают во взаимодействии с ними. Сообщить о негативном контенте на «Горячую линию» (в отличие от правоохранительного органа), как правило, можно анонимно. Для отправки сообщения надо скопировать из браузера и вставить в окно «Горячей линии» ссылку на «подозрительный» сайт и указать, к какой категории этот сайт, по Вашему мнению, относится.

Все сообщения, поступившие на «Горячую линию», обязательно проверяются опытными аналитиками – специалистами по контенту в Интернете. Они могут профессионально определить, является ли этот контент потенциально противоправным в соответствии с российским законодательством, или нет. Для прекращения оборота противоправного контента в «Горячей линии» предусмотрен ряд процедур, включающих в себя взаимодействие с провайдерами и правоохранительными органами. Прекращением оборота противоправного контента процедуры, как правило, не заканчиваются – правоохранители устанавливают личность злоумышленника и привлекают его к установленной законом ответственности.

ПРАВИЛА БЕЗОПАСНОСТИ В России действует «Горячая линия» Центра безопасного Интернета. Она принимает сообщения по девяти категориям опасного контента и входит в международную сеть таких же «горячих линий» в разных странах - INHOPE. Таким образом, размещение контента вне российской юрисдикции в данном случае, как правило, не представляет проблемы для того, чтобы прекратить его оборот.

Если Вы встретились с потенциально опасным для ребенка или противоправным контентом (как, например, киберунижение или детская порнография) – обязательно сообщите о нем на «Горячую линию»! Этим Вы защитите и себя, и других пользователей Сети. При этом крайне не рекомендуется привлекать несовершеннолетних к поиску противоправного контента.

ГРУМИНГ (от английского grooming) – так называют действия педофилов по поиску и завлечению своих жертв через Интернет. Педофил знакомится с ребенком в социальной сети, в чате, на форуме, через электронную почту; не являются полностью безопасными даже чисто «детские» ресурсы, так как опытный злоумышленник легко может «подстроиться» под стиль общения ребенка. При этом педофил в общении может представляться как взрослым, так и ребенком. После установления контакта он начинает всячески входить в доверие к ребенку или подростку – конкретные стратегии преступников зависят от возраста ребенка, его жизненной ситуации, потребностей и т.п. Завоевав доверие, злоумышленник предпринимает шаги к сексуальной эксплуатации несовершеннолетнего – например, просит переслать ему свои фото или видео в обнаженном виде, либо доби-

вается реальной встречи с ребенком в целях вступления с ним в половую связь или похищения.

ПРАВИЛА БЕЗОПАСНОСТИ Главное правило безопасности при онлайн-коммуникации очень простое: виртуальный друг должен оставаться виртуальным. В Сети очень легко создать и поддерживать «ложную идентичность», поэтому собеседник может представиться кем угодно: хоть старушкой, хоть известным киноактером, хоть ожившим персонажем мультфильма. В связи с этим обязательным правилом для ребенка должно стать сообщение родителям о своих «виртуальных контактах» и избегание встреч с ними «в реале». В крайнем случае такая встреча может пройти под наблюдением родителей.

Если виртуальный «друг» начинает вести себя с заведомым для него ребенком в Сети непристойно – например, побуждать к сексуальным действиям, пересылать посты и фото непристойного характера, заводить беседы на сексуальные темы – ребенку следует ОБЯЗАТЕЛЬНО прервать общение с таким «другом» и рассказать о нем родителям. В ситуации, если такой собеседник знает, что беседует с несовершеннолетним, и тем не менее переходит на «сексуальное» общение, крайне высока вероятность того, что «по ту сторону экрана» сидит настоящий педофил.

ГУГЛБОМБИНГ (по-английски Googlebombing, также используется термин link bomb – «бомбежка ссылками») - специальная хакерская шутка, влияющая на результаты поисковых выдач. Суть ее в том, что хакер подменяет запрос в поисковике тем результатом, который ему нужен, и первым в списке может выходить интересный ему сайт – или сайт, которому он хочет отомстить. Например, набирая фразу «большее зло, чем сам сатана», пользователь попадал на сайт компании Microsoft. Таким образом, получалось, что «большее зло» и есть компания Microsoft.

Чтобы устроить подобную «шутку», хакеры пользуются специальными компьютерными программами, которые оценивают Интернет-страницы – точнее, количество и популярность разных сайтов, которые поисковик выдает в ответе на некий запрос. Так «шутники» специально используют задуманные ими фразы как ссылку на необходимый сайт, чтобы таким образом поднять позиции сайта по данным запросам – или, наоборот, кого-то унизить.

Гуглбомбинг относительно безобиден по сравнению с вредоносным вторжением, но тем не менее может негативно влиять на репутацию некоего сайта. Впрочем, гуглбомбинг используется и в целях «вирусной рекламы» некоего сайта или продукта.

ПРАВИЛА БЕЗОПАСНОСТИ Источник «враждебной» ссылки можно узнать, используя функции поисковых систем. Например, если ввести нужный запрос в кавычках в Яндексе, поисковик выдаст всех пользователей, кто использовал именно это слово или фразу. Но источник ссылки проще определить, если фраза длинная и уникальная.

Д

ДЕТСКАЯ ПОРНОГРАФИЯ - фотографии, видеоролики или тексты, где дети и подростки вовлечены в совершение сексуальных действий, очень часто со взрослыми. Часто для этого детей обманывают или запугивают, а иногда и просто насилуют. Более «научное» название – «Сцены сексуальной эксплуатации несовершеннолетних».

Детская порнография представляет собой угрозу в первую очередь против чести, достоинства и репутации жертвы, хотя с точки зрения ряда юристов она является также длящимся преступлением против половой неприкосновенности. Жертва сексуальной эксплуатации может подвергаться унижению, насмешкам в связи с совершенным в отношении нее преступлением. Даже простое обсуждение свидетельствует о том, что о факте знают посторонние, что также крайне негативно воздействует на жертву и может стать причиной самоубийства.

Дополнительную опасность составляет трансграничность Интернета – подобный контент, произведенный в одной стране, может быть опубликован в другой и доступен для просмотра по всему миру.

ПРАВИЛА БЕЗОПАСНОСТИ Если Вам встретились сцены с детской порнографией в Сети – немедленно примите меры к пресечению его оборота, сообщив о ней на «Горячую линию» или на Правоохранительный портал.

Нередко сексуальная эксплуатация несовершеннолетних осуществляется прямо через Интернет: педофил просит ребенка совершить некие сексуальные действия перед веб-камерой своего компьютера (или даже смартфона), записывает видео и затем распространяет через Интернет – либо начинает шантажировать распространением этого видео или фото, требуя все новых сексуальных действий перед веб-камерой, а то и просто денег. Поэтому, если виртуальный собеседник ребенка просит сделать что-то непристойное перед компьютером или камерой (например, раздеться) – ребенок должен знать, что этого делать ни в коем случае нельзя. Никакая кажущаяся «популярность» не окупает рисков, о чем свидетельствует история ряда голливудских кинозвезд от Деми Мур до Брук Шилдс. Если же просьба о подобных действиях все же поступила, ребенку или подростку следует немедленно сообщить об этом родителям.

ДОМЕН (от английского domain – область, поле деятельности) - это то, что мы привыкли считать адресом сайта. Строго говоря, домен - это буквенное обозначение адреса сайта, более привычное и удобное по сравнению с IP-адресом, который записывается в цифрах. Пример: IP-адрес - 123.456.78.90, доменное имя - microsoft.com.

Кроме того, доменное имя сайта способно сразу сообщить о нем много дополнительной информации. К примеру, окончание доменного имени может дать представление о его географической принадлежности (.ru – российские сайты, .ua – украинские, .ca – Канада, de. – Германия и т.п.), а так же цели создания - .com (коммерческий), .org (некоммерческие организации). Сейчас появились доменные зоны, не имеющие привязки к стране или цели создания – после точки может идти название города (.moscow), тематики (.kids) или вообще компании (.yandex). В настоящее

время доменное имя может писаться не только латинскими буквами, но и буквами других алфавитов – например, кириллическим (как в домене .рф).

Как правило, домен является «визитной карточкой», «брендом» сайта – сайт узнается пользователями именно по доменному имени.

ПРАВИЛА БЕЗОПАСНОСТИ При посещении неизвестного Вам сайта обращайте особенное внимание на правильное написание его доменного имени. Известны случаи, когда мошенники, заменив в имени сайта несколько букв или символов, заводили людей на «поддельные» сайты – например, чтобы продать что-нибудь от имени известной фирмы. В России, например, был случай, когда мошенники создали сайт-двойник, на котором от имени популярной телевизионной ведущей рекламировалась «чудодейственная» диета. Сайт выглядел в точности как настоящий, но адрес у него был другой. Итог – потеря денег со стороны пользователей.

Е

Е-МЕЙЛ - (английское email, e-mail, от electronic mail) – электронная почта. Преимуществом электронной почты является прежде всего скорость передачи сообщений – письмо приходит почти мгновенно. Также в электронной почте есть возможность пересылать не только текст, но и прикрепить к письму другие файлы, например картинки.

Адрес электронной почты состоит из трех частей. Первая часть – индивидуальное (то есть личное) имя, выбранное для почты самим пользователем. Не забывайте о том, что оно должно быть корректным, удобным для написания и запоминания. Вторая – символ «@» (англ. – at, «the at sign»), который является отличительным знаком адреса электронной почты. В России его традиционно называют «собака», в Швеции – «слон», в Турции – «розочка». Третья часть сообщает, на какой именно почтовой службе размещен этот адрес. Например, info@nedopusti.ru значит, что адрес info привязан к почтовой системе сайта nedopusti.ru.

ПРАВИЛА БЕЗОПАСНОСТИ Мошенники очень часто используют для спамерских атак и рассылки вирусов именно электронную почту. Поэтому старайтесь не оставлять свой адрес электронной почты на всех сайтах и сервисах подряд. Если для регистрации на сайтах вам требуется его указать, всегда лучше создать дополнительный временный адрес. Кроме того, никогда не открывайте вложения, присланные с неизвестных Вам или подозрительных адресов – в подавляющем числе случаев Вы рискуете получить компьютерный вирус!

Ж

ЖЖ, ЖЭЖЭ, ЖЕЖЕШЕЧКА – популярный сервис блогов LiveJournal («Живой Журнал»). Блог - (англ. blog, от web log — интернет-журнал событий) - это интернет-дневник, личная интернет-газета, которую может выпускать каждый – и при этом общаться с читателями. Отличие блога от страницы в социальной сети или персонального сайта состоит в том, что главным элементом блога являются тексты. Размещаются они обычно по принципу новизны: чем новее текст, тем он выше. Кроме того, ведение блога в сети Интернет предполагает его публичность – то есть его кто-то читает и даже комментирует (пишет

свои мысли в ответ).

К слову, блоги имеются не только у людей – но и у сообществ и даже у юридических лиц: компаний и организаций. Такие блоги служат целям пиара и рекламы, рассказывают о достижениях компании, интересных предложениях и т.п., и могут вестись сразу несколькими сотрудниками. Впрочем, бывает и так, что несколько человек могут вести блог, считающийся персональным – например, после домашнего ареста оппозиционера Алексея Навального, по некоторым утверждениям, блог от его имени ведут его единомышленники.

ПРАВИЛА БЕЗОПАСНОСТИ Поскольку блог могут читать многие, сначала надо подумать, и только потом написать. Если можно сделать блог видимым только для друзей, лучше сделать именно так – это еще одно средство безопасности от сетевых хулиганов.

З

ЗАПОСТИТЬ (от английского to post)– написать в Интернете сообщение. Обычно это выражение употребляется в блогах, на форумах и в сообществах. Также оно применяется, когда речь идет о любом тексте, изображении, видео, выкладываемом в Сеть.

С размещением сообщений в Сети (особенно, если это касается форумов) связано понятие «треды» (англ. thread — «нить»), то есть «ветви» обсуждения. Когда пользователю доступна возможность отвечать на сообщение другого пользователя, комментировать его, этот ответ «привязывается» к посту. Так как делать это можно практически бесконечно, ветви обсуждения могут быть очень «раскидистыми».

ПРАВИЛА БЕЗОПАСНОСТИ Не забывать о том, что если Вы хотите донести свою мысль или отношение к какой-то теме до читателя (а ведение онлайн-дневника подразумевает именно это) – Ваш пост должен быть интересным, грамотным, не должен содержать оскорбительных высказываний. Если Вы состоите в каком-то сообществе – пишите по теме, не стоит портить о себе впечатление, прослыв «троллем» или «флудильщиком».

И

ИНТЕРНЕТ-ЗАВИСИМОСТЬ (по-английски Internet-addiction) – состояние, когда человек чувствует сильное желание как можно больше времени проводить в Интернете и очень болезненно переживает моменты, когда не может туда попасть. Бывает, что интернет-зависимые люди сидят в Сети сутками и даже умирают от этого. Зачастую им необходим сам процесс пребывания в Интернете, то есть они могут просто бесцельно бродить по различным сайтам.

Некоторые врачи считают, что Интернет-зависимость – это разновидность психической патологии, то есть психическое заболевание. Впервые о нем упомянул в 1995 году доктор Иван Голдберг, который в описании сравнил его с последствием злоупотребления психоактивными веществами – например, зависимостью от наркотиков. Сейчас психиатры различают 5 основных типов Интернет-зависимости: бесконечные «путешествия» по Сети, навязчивое общение в Интернете, страсть к компьютерным играм, играм на день-

ги или порносайтам.

ПРАВИЛА БЕЗОПАСНОСТИ Интернет-зависимость часто «настигает» подростков, которые не находят в реальном мире достаточно увлечений и общения - и потому ищут «убежище» в Сети. Нужно всегда помнить: Интернет – это не замена реальному миру, это всего лишь помощник для реального мира! От долгого сидения в Интернете начинают появляться вполне настоящие болезни - от проблем с социализацией до вполне физиологических.

Родителям следует знать, что лучшее средство избежать интернет-зависимости - наладить контакт с ребенком в семье, увлечь его другими хобби и разъяснить, что «путешествия» в киберпространстве – такое же удовольствие, как и прогулки на свежем воздухе, игры с реальными друзьями, чтение интересной книги и так далее. Если ребенок стал киберзависимым, нужно обратиться к психологу – он поможет увидеть проблему и разобраться с ней. Здесь не следует отождествлять психолога с психиатром – речь идет о совершенно разных специалистах, с разными формальностями и разными юридическими последствиями, которых Вы можете опасаться от психиатра (например, на «учет» в психдиспансер Вас и Вашего ребенка никто не поставит).

К ***КИБЕРУНИЖЕНИЕ*** (от английского cyberbullying) – преследование и унижение кого-то в Интернете или по мобильному телефону.

Бывает два вида киберунижения. «Классическое» - когда жертву начинают «заваливать» оскорблениями, насмешками или угрозами по всем ее электронным контактам: по электронной почте, в социальной сети, блоге, СМС. Второй вид киберунижения – когда кто-то снимает издевательства или унижения на камеру и выкладывает это в Интернет или рассылает через мобильники. Особо циничные проекты по киберунижению могут иметь «социально значимый», научный или даже медицинский антураж.

ПРАВИЛА БЕЗОПАСНОСТИ Помните, что очень часто своими действиями пользователи сами дают возможность хулиганам и преступникам найти их «слабые места». Поэтому не публикуйте открыто свои контакты: домашний адрес, номер мобильного или домашнего телефона, адрес электронной почты, не выкладывайте фотографии, на которые легко написать издевательский комментарий, не будьте излишне доверчивы и не торопитесь рассказывать незнакомцу всю свою биографию (жизненную историю).

Практически на всех форумах и сайтах, где есть возможность общаться, существует функция, позволяющая заблокировать «нехорошего» пользователя. В крайнем случае, не так трудно удалить свою анкету с сайта знакомств или из социальной сети, чтобы не быть больше мишенью для оскорблений и травли. Кроме того, Вы всегда можете найти управу на обидчиков, сообщив администрации сайта, или написав заявление в полицию (ведь киберунижение – это серьезное преступление!). Если дело происходит в школе – обязательно надо дать знать учителю. Это не «стукачество», а самозащита!

Удалить сцены киберунижения из Сети можно, обратившись на Горячую ЛИНИЮ.

КРЯК (от английского crack - сломать, взломать) – специальная хакерская программа, позволяющая «активировать» (то есть включить) лицензионную программу, не заплатив за нее. После «кряканья» лицензионная программа считает, что ее законно активировали и что за нее заплатили. Обычно эта программа «изображает» лицензионный ключ – код для активации программы.

Использование этих программ является прямым нарушением авторских прав - за них можно понести реальную ответственность. Но есть и другая беда: «кряки» - очень серьезный источник заражения вирусами, так как под них часто маскируют вирусы и другие опасные программы.

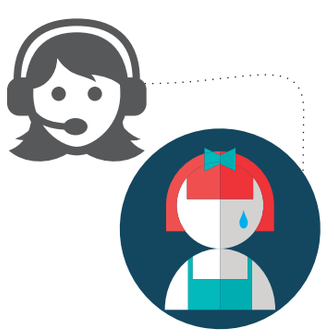
КУКИ (от английского cookie — печенье) - файлы небольшого размера, которые хранятся в специальной папке браузера и сохраняют информацию о пользователе при посещении им сайтов. В частности, в них могут сохраняться учетные записи и пароли к ним, имена (ники) пользователя, его электронный адрес и так далее. Это словечко придумала компания Netscape – когда-то один из главных производителей браузеров.

Эта возможность удобна для пользователя тем, что при каждом открытии сайта ему не приходится заново набирать свои данные. С другой стороны, это удобно и для сервера – на нем не надо занимать место, сервер получает всю информацию о пользователях прямо с их компьютеров. Однако есть и минус – куки формируют своеобразное «Интернет-досье» на пользователя компьютера. Если что, куки на своем компьютере можно стереть – любой браузер дает такую возможность.

ПРАВИЛА БЕЗОПАСНОСТИ Информация, которая находится в **COOKIE** –файлах, может быть использована в мошеннических целях или просто похищена. Поэтому современные браузеры позволяют отключать создание «**КУКОВ**».

«ЛИНИЯ ПОМОЩИ» - специальная служба, по которой можно получить совет, как быть и что сделать для своей безопасности в Интернете. Специалисты подскажут каждому обратившемуся по той ситуации, которая возникла именно у него. Если кто-то пострадал от Интернет-злоумышленников, ему помогут психологи.

На «Линию помощи» можно написать в Интернете (на сайт или пообщаться в чате), а можно позвонить по телефону.



ПРАВИЛА БЕЗОПАСНОСТИ Если Вы что-то не знаете или в чем-то сомневаетесь насчет своей безопасности в Сети – не стесняйтесь обратиться на «Линию помощи». Это удобно и бесплатно. Особенно если Вы стали жертвой Интернет-угрозы – на «Линии помощи» смогут помочь комплексно и профессионально.

В России работает «Линия помощи» Центра безопасного Интернета в России. Ее телефонная часть входит в общероссийский проект «Телефон доверия», куда можно бесплатно позвонить по телефону 8-800-2000-122. Через Интернет со специалистами «Линии помощи» можно пообщаться при помощи сайта Центра безопасного Интернета nedopusti.ru.

ЛОГИН – (по-английски log in) - имя, которое Вы выбираете для регистрации на сайте или просто на компьютере. Иногда система или компьютер может присвоить логин сама, но это бывает редко и его обычно можно поменять на тот, который Вам больше нравится. Каждый пользователь в системе имеет свой уникальный логин. Он помогает системе и другим пользователям отличить одного пользователя от другого.

Если Вы забыли свой логин или пароль, Вам не обязательно регистрироваться заново. Достаточно в нужную форму вписать адрес своего почтового ящика (электронной почты), который Вы использовали при регистрации. После ввода в форму адреса ящика Вы получите письмо со своими регистрационными данными на этот ящик.

Зная логин и пароль или имея доступ к нужному аккаунту, можно получить доступ ко всему остальному, поэтому мошенники очень часто практикуют взлом аккаунтов.

ПРАВИЛА БЕЗОПАСНОСТИ Не забывайте логин и пароль от своего аккаунта, так как все дороги к другим ресурсам ведут от него. Старайтесь придумать сложные пароли для разных площадок общения, не дублируйте их, не храните на компьютере, иначе Ваш аккаунт может быть взломан.

МОДЕРАТОР (латинское moderator, от moderor — умеряю, сдерживаю) – пользователь, который присматривает за порядком в любом сообществе и на форуме. Обычно модератором назначается активный пользователь какого-либо форума, блога или другого ресурса в Интернете, где участники активно общаются между собой – либо модераторские функции выполняет хозяин ресурса. Он наделен особыми правами по сравнению с остальными пользователями – может править чужие посты, выносить предупреждения или банить Интернет-хулиганов. На «любительских» Интернет-площадках он обычно за это денег не получает – а вот на коммуникационных площадках сайтов компаний, газет и т.п. для модерирования нанимаются специальные люди, то есть они работают за зарплату. На каждом форуме или сообществе существуют правила, за соблюдением которых и следит модератор.

ПРАВИЛА БЕЗОПАСНОСТИ Модераторы выполняют функции «фильтров», которые стремятся сделать так, чтобы в сообществе всем было интересно, удобно и безопасно общаться, так что будьте уважительны к их замечаниям. Если Вам поступило предупреждение, отреагируйте на него с пониманием и учтите, как надо себя вести.

Если в отношении Вас кто-то нарушил правила форума или сайта, то нужно обратиться именно к модератору. Бывает, что и сам модератор не лучше Интернет-хулигана (например, «покрывает» неподобающие действия другого пользователя) – тогда лучше просто уйти с такого сайта. Потому что похожих сайтов много, а модераторы на других сайтах могут быть лучше.

НУБ - (от английского newbie — новичок). Изначально слово обозначало человека, не освоившегося в Интернете, в частности на форумах и конференциях, в онлайн-играх. Плотно вошло в лексикон геймеров.

Сейчас слово «нуб» означает назойливого игрока, не желающего подчиняться общим правилам. То есть ничего хорошего оно не несет и является насмешливым. Еще нубом называют человека, который не пытается найти ответ на свой вопрос через поиск на форуме, а создает тему, копируя по невнимательности уже существующие. Не случайно самый популярный совет от опытных игроков нубу звучит так: «Учи матчасть!» (эта фраза – из знаменитого фильма про войну «В бой идут одни старики»).

ПРАВИЛА БЕЗОПАСНОСТИ И все-таки «нуб» - это оскорбление, со всеми вытекающими результатами. Поэтому как быть в таком случае, можно узнать из статей «Модератор» и «Киберунижение».

ОФФТОПИК - (по-английски off topic - вне темы)

Обычно оффтопиком пользователи Сети называют запись, которая совершенно не соответствует теме общения (на веб-форуме, в блоге и т.п.), или сообщение «не по делу» в уже существующей теме. Модераторы относятся к оффтопикам крайне негативно, так как их появление может запутать других пользователей, а то и вовсе отпугнуть их от посещения «загрязненного» лишней информацией ресурса.

ПЕДОФИЛ – взрослый человек (обычно имеющий приличную разницу в возрасте со своей жертвой), который хочет совершать или совершает сексуальные действия с детьми и подростками. Строго говоря, с медицинской точки зрения именно педофилами являются те, кто испытывает сексуальное влечение к детям, не достигшим подросткового возраста, а «любителей» подростков (теоретически вступающих в возраст полового созревания) наука называет эфебофилами. Однако благодаря прессе слово «педофил» прочно приклеилось ко всем тем, кто хочет совершить или совершает сексуальные действия с несовершеннолетними вообще, независимости от их пола и возраста.

С распространением Интернет-технологий педофилы очень быстро оценили их «достоинства» для себя, позволяющие минимизировать риски поиска детей в оффлайне – и часто стремятся искать своих жертв в Интернете. Надо сказать, что они делают это очень изобретательно – выдают себя за таких же детей и подростков, известных певцов и актеров, благотворителей и так далее. Своих жертв педофилы ищут в социальных сетях, на форумах, в чатах, могут познакомиться даже по электронной почте. Как они это делают, можно прочитать в статье «Груминг».

Буквально «педофил» переводится с греческого как «тот, кто любит детей». Но их «любовь» полностью ломает жизнь детям и подросткам.

Целью педофила, как правило, является получение сексуального удовлетворения от тех или иных действий с ребенком (от сексуального общения до собственно секса). Съемки детской порнографии для них – скорее сопутствующее действие, которым они стараются запечатлеть сексуальную эксплуатацию, чтобы потом прокручивать видео или просматривать фото снова и снова. Однако они нередко делятся результатами «съемок» между собой, создавая таким образом оборот сцен сексуальной эксплуатации детей. Есть и «предприимчивые дельцы», которые наладили целый бизнес по производству таких порнографических фото или видео. Хотя актеры в таких фильмах могут и не испытывать физиологического влечения к детям, с точки зрения закона и морали они все равно рассматриваются как педофилы.

ПРАВИЛА БЕЗОПАСНОСТИ Если у ребенка возникло ощущение, что его «виртуальный друг» - педофил, то он должен немедленно сообщить родителям, учителю или на «Горячую линию». Педофил может быть очень жесток – и всегда опасен! Однако нужно предостеречь ребенка от рассказывания всем о своем контакте с педофилом – все могут понимать это по-разному.

Родителям крайне целесообразно быть в курсе Интернет-знакомств ребенка – именно с целью раннего выявления опасных для ребенка контактов и избежания опасных последствий. Однако делать это через «допросы» ребенка или, еще хуже, тайно отслеживать переписку чада категорически не следует – ребенок немедленно примет меры к «засекречиванию» своей Интернет-жизни, а контакт с родителями окончательно подорвется. Наилучшим вариантом является наличие глубокого уровня доверия в семье и понимание ребенком потенциальной опасности от Интернет-контактов – тогда ребенок сам будет стремиться к сотрудничеству с родителем и Вы будете в курсе «виртуальной» стороны его жизни.

ПРОВАЙДЕР (по-английски Internet Service Provider, ISP, букв. "поставщик Интернет-услуги") - это та фирма, которая обеспечивает Интернет или какие-то его сервисы.

Под словом «провайдер» могут скрываться организации, оказывающие совершенно разные типы услуг – их дифференцируют по их полному названию:

ХОСТИНГ-ПРОВАЙДЕР – это тот, кто предоставляет услугу размещения на своих серверах сайтов, то есть тот, у кого эти сайты хранятся. Нередко он называется просто «хостер».

КОНТЕНТ-ПРОВАЙДЕР – он «обеспечивает» нас контентом, что-то публикует. Разновидность контент-провайдера – фотохостинги и видеохостинги, то есть службы, на которых можно выкладывать свои фото или видео. К контент-провайдерам иногда относят и социальные сети.

ИНТЕРНЕТ-ПРОВАЙДЕР – это тот, кто обеспечивает нам возможность собственно соединяться с Интернетом через провода или мобильники.

ПРАВИЛА БЕЗОПАСНОСТИ Если Вам попался сайт с «нехорошим» контентом, то можно обратиться и к провайдеру. У некоторых провайдеров существуют свои «абьюз-тимы» (команды по конфликтам), которые специально существуют для приема жалоб пользователей и принимают по ним меры.

ПРАНК – (по-английски prank — проказа, выходка, шалость) — телефонное хулиганство, розыгрыш, который пранкер записывает и выкладывает потом в Интернете. Шутники звонят (обычно анонимно) своей «жертве» и путём травли вынуждают ее к яркой ответной реакции (грубости, нервному срыву) – это их забавляет. Пранк-культура, равно как и сам термин «пранк», появились в России на рубеже XX—XXI веков, хотя само телефонное хулиганство присутствует в нашей стране уже лет девяносто.

ПРАВИЛА БЕЗОПАСНОСТИ Пранк – это не шалость, а преступление, и за него можно ответить по закону. Ребенок должен знать, что «телефонным хулиганством» заниматься ни в коем случае нельзя и тем более нельзя выкладывать такие записи в Интернет!

Если Вы или Ваш ребенок сами стали жертвой такого хулигана, то помните: его главная задача – устроить ссору. Поэтому просто старайтесь не реагировать на подобные звонки. Лучшим способом испортить хулигану его выходку может стать Ваш отказ от попыток завязать с вами беседу. Лучше всего – прервите сразу любой подозрительный разговор. Если пранкеры «достают», можно вообще сменить номер телефона.

РУНЕТ — виртуальное пространство России.

Название «Рунет» образовалось из доменного имени .ru и постфикса net (дословно «русская сеть») и вошло в употребление в конце 1990-х годов.

Говорят, что термин придумал в 1997 году автор одной из первых регулярных русскоязычных сетевых колонок Раффи Асланбеков и стал использовать его в своем общении. Новое слово прижилось и попало даже в словари.

Что интересно, похожим образом стали называть и некоторые другие сегменты (зоны) Интернета, относящиеся к странам бывшего СССР: в Казахстане Интернет стали именовать «Казнет», в Белоруссии «Байнет», в Украине — «УАнет», в Узбекистане — «Узнет» и подобное.

Существует «Премия Рунета» — ежегодная Национальная премия за вклад в развитие российского сегмента сети Интернет.

РПГ - (по-английски Computer Role-Playing Game (CRPG или RPG) – в Интернете это означает не гранатомет, а компьютерную ролевую игру. В ней пользователь может играть от имени одного героя или от группы героев. Как правило, суть игры состоит в том, что выполняя квесты (задания, которые по сюжетной линии даются основными или дополнительными игровыми персонажами), герой повышает свой уровень и имеет возможность развивать свои характеристики, улучшать броню и оружие и так далее. Обычно в этом случае пользователь играет напрямую «с компьютером».

Есть еще ММОРПГ (по-английски massively multiplayer online role-playing game) – это уже игра для большого количества игроков. Здесь человек играет не с компьютером, а с другими людьми - что вносит в нее важные дополнения. Первое –

игровой процесс движется, даже если пользователь в данный момент не находится онлайн. Второе – возникают вопросы, связанные с внутриигровым общением и взаимодействием всех геймеров.

ПРАВИЛА БЕЗОПАСНОСТИ Несмотря на то, что процесс игры бывает очень увлекательным и может «затянуть» надолго, не забывайте, что все хорошо в меру. Находя время на игру, не отказывайтесь абсолютно от реальной жизни, ведь и в ней есть очень много интересного и полезного. Учитесь соблюдать «золотую середину». И помните, что даже если на мониторе Вы видите совершенно фантастического персонажа, в жизни это – такой же человек, как Вы. Поэтому в играх обязательно следует соблюдать правила поведения, не грубить, не мешать играть другому человеку, не нарушать законы игрового мира. Эти правила ребенок должен четко помнить – они помогут его качественной социализации.

СПАМ (сокращение от англ. «spiced ham» - ветчина со специями). Интернет-пользователям это слово хорошо знакомо как обозначение сообщений (особенно по электронной почте, а также в социальных сетях или по СМС), которых они не просили и не ожидали. Спам носит в основном рекламный характер и опасен тем, что буквально «забивает» почтовый ящик, не давая пользователю возможности нормально пользоваться своей почтой. Спам может просто «завесить» почтовый ящик. Кроме того, очень часто в спам-рассылке приходят «замаскированные» вирусы. Спамом также пользуются Интернет-мошенники для рассылки привлекательных «предложений» - например, купить нечто с огромной скидкой, получить выигрыш в лотерею или помочь «наследнику свергнутого диктатора» за некое вознаграждение заполучить оставленное наследство (так называемые «нигерийские письма»).

ПРАВИЛА БЕЗОПАСНОСТИ Спамеры рассылают свои письма без какой-то определенной системы, добывая адреса электронной почты из баз данных почтовых серверов или Интернет-магазинов. Кроме того, они смотрят любые «открытые» площадки в Сети – «доски объявлений», форумы, чаты и так далее, а также просто подбирают самые легкие, часто использующиеся и «красивые» адреса. Поэтому очень важно не оставлять свой постоянный адрес электронной почты везде, где этого могут попросить. Создавайте разовые адреса для каждого случая. А если пришлось «выложить» адрес в публичном доступе, воспользуйтесь несложной хитростью – записывайте адрес только буквами, например: «Вася-собака-mail-точка-ру». Это собьет с толку автоматических роботов - сборщиков адресов, которыми пользуются спамеры.

Обязательно нужно соответствующим образом настроить свою почтовую программу – в каждой из них есть защита от **СПАМА**. Можно «помочь» программе, создавая «белые» и «черные» списки адресов электронной почты – так, например, можно избавиться от киберунижения по E-mail. И обязательно надо сканировать входящие письма антивирусом - чтобы не получить прикрепленный «подарок» в виде вируса или трояна.

СЕКСТИНГ - (от английского sex + texting) - отправка электронных сообщений или изображений сексуального характера по Сети или мобильному телефону.

Обычно этим увлекаются подростки и молодежь, которые снимают себя сами. В секстинге они видят некий способ самовыражения, привлечения внимания, своеобразный вызов обществу, ведь такие фотографии точно не останутся незамеченными. Кто-то воспринимает это как интересную игру, кому-то это дает ощущение «звездности», для кого-то секстинг - просто веселье и забава.

По мнению некоторых психологов, к секстингу можно пристраститься как к наркотику: выставляя свои фотографии в социальных сетях, подростки рано или поздно замечают, что самой большой популярностью пользуются те из них, где они сняты полуобнажёнными. Соответственно, это стимулирует их к производству и публикации все более и более «откровенных» собственных изображений.

Секстинг опасен тем же, чем опасно любое неосторожное изображение эротического или порнографического характера: угрозой чести и достоинству личности, а иногда и физической безопасности. К примеру, очень часто такие «интимные селфи» расползаются по ресурсам педофилов, а то и просто по «сайтам знакомств». Часто публикация такого изображения вызывает в «ближнем кругу» общения не популярность, а насмешки; может поменяться в негативную сторону характер общения с автором секстингового изображения.

ПРАВИЛА БЕЗОПАСНОСТИ На определенном этапе взросления с ребенком понадобится соответствующая работа, в результате которых он должен будет усвоить допустимые и недопустимые методы поиска «популярности». В частности, ему (да и многим взрослым) следует помнить, что по соображениям безопасности никогда нельзя отправлять или выкладывать в Интернет свои фото или видео в обнаженном, полуобнаженном или вообще непристойном виде! Последствия могут быть весьма трагичны: откровенные фотографии могут попасть в руки родителей, учителей, членов приемных комиссий учебных заведений, потенциальных работодателей и «сыграть» против изображенного там персонажа даже через много лет. Так, например, случалось со знаменитыми актерами и актрисами, кто начинал свою карьеру в «фильмах для взрослых».

Но самая опасная сторона секстинга в том, что ребенок, сам того не осознавая, может спровоцировать педофилов на преступные действия.

СЕРВЕР – большой компьютер, при помощи которого «раздают» Интернет или на котором хранится информация в Интернете.

ПРАВИЛА БЕЗОПАСНОСТИ Атака на серверы может «завесить» многие Интернет-ресурсы. Поэтому в серьезных компаниях серверы очень хорошо защищены.

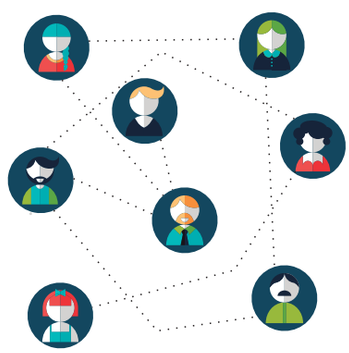
СМАЙЛ - значок в Сети, с помощью которого можно выражать эмоции и передавать настроение. Когда смайлики только входили в моду, многие в недоумении ломали голову – что это за странные скобки и двоеточия в конце предложения? Позже они стали настолько популярны, что сейчас без них не обходится ни одна переписка не только в Интернете, но и в мобильных телефонах.

Существует множество вариантов смайликов, вот некоторые из них:

:-) УЛЫБАЮСЬ
;-) ПОДМИГИВАЮ
:-O УДИВЛЯЮСЬ
:(ГРУЩУ
:`-(ПЛАЧУ
:-P ПОКАЗЫВАЮ ЯЗЫК
:-D ХОХОЧУ
:-* ЧМОК!
}:-) ХМУРЮСЬ
^_^ ЯПОНСКАЯ УЛЫБКА

ПРАВИЛА БЕЗОПАСНОСТИ Смайликом тоже можно оскорбить. Поэтому думайте, какой смайлик или символ Вы ставите в тексте.

СОЦИАЛЬНАЯ СЕТЬ – специальный сайт, который дает больше всего возможностей «рассказать о себе». У каждого пользователя есть своя страничка, где он рассказывает о себе, помещает свои фото и видео (а также те видео, что ему понравились), «френдит» (то есть заводит) друзей, переписывается с ними. По сути, социальная сеть объединяет в себе функции форума, чата, видеохостинга, персонального сайта и гостевой книги. В некоторых социальных сетях можно создавать странички сообществ (например, по увлечениям), играть в онлайн-игры и делать много других интересных вещей.



ПРАВИЛА БЕЗОПАСНОСТИ К сожалению, именно в социальных сетях многие Интернет-хулиганы и преступники делают свои черные дела. Взламывают странички других пользователей и размещают на них непристойную информацию, просто публикуют опасный контент (например, сцены унижения сверстников), собирают данные для совершения преступлений, рассылают спам, ищут будущих жертв. Это особенно опасно потому, что на социальные сети приходит очень много народа и очень много людей могут стать жертвами таких опасных действий.

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ ДЛЯ СОЦИАЛЬНЫХ СЕТЕЙ (подходящие и детям, и взрослым) таковы:

- Следует хорошо подумать, прежде чем что-то написать или опубликовать в Интернете. Непродуманный пост может подсказать хулиганам и преступникам, как лучше причинить вред его автору или близким.

- Нельзя выкладывать в социальной сети личную информацию и тем более личные фотографии. Необходимо помнить: все, что ты выложил в сети, увидят другие. А что они с этим сделают – вопрос…

- Не следует «френдить» всех подряд. Дружить в социальных сетях нужно только с проверенными в «реале» друзьями. Обычно другу в социальной сети можно видеть больше, чем обычному гостю, так что мера предосторожности не лишняя.

- Ни в коем случае нельзя публиковать в социальной сети то, что может обидеть и унизить других пользователей или просто других людей! Даже в шутку – такие «шутки» плохо кончаются.

• Очень рекомендуется проверять антивирусом все присылаемые «приложения».

• Крайне не рекомендуется играть в социальной сети на деньги и запускать приложения, требующие денег за участие или поднятие в них своего «статуса». Для ребенка же подобные действия являются просто недопустимыми.

• Если пользователь стал жертвой оскорблений или опасного контента – он может обратиться за помощью к администратору социальной сети или на «Горячую линию».

ТОРРЕНТ – (по-английски torrent – поток) - сервис обмена файлами между людьми в Интернете. Передаваемый файл не загружается на сервер, а напрямую передается от пользователя к пользователю. В тот момент, когда на компьютер скачивается файл, он одновременно раздается другим пользователям – это обеспечивает постоянный доступ к файлам и оперативность скачивания. На сегодняшний день такая система обмена контентом является одной из самых популярных, и ею пользуются миллионы людей по всему миру. Но бесплатное скачивание лицензионных материалов через трекеры является нарушением авторских прав, поэтому торренты очень «не любит» полиция. Например, в России 18 февраля 2010 года прокуратура лишила крупнейший торрент-трекер Torrents.ru его доменного адреса.

ПРАВИЛА БЕЗОПАСНОСТИ Нарушать авторские права, конечно же, нехорошо. Поэтому скачивайте лицензионную продукцию с лицензионных сайтов.

ТРОЛЛИНГ – провокация собеседников в Интернете.

ТРОЛЛИНГОМ, само собой, занимаются тролли. Их так называют потому, что сказочные тролли очень уродливы и противны в общении. Уже из этого описания следует, что троллей в Интернете, мягко говоря, не любят. Тролли получают удовольствие от негативной (то есть плохой, резкой) реакции других людей - поэтому они намеренно идут на провокации в общении и доводят собеседника до нервного срыва, который выплескивается в онлайн.

Обычно ТРОЛЛИНГОМ любят заниматься подростки – так они «самовыражаются». Однако в сообществах встречаются и вполне взрослые профессиональные Интернет-скандалисты, для которых «довести» виртуального собеседника является своего рода искусством.

ПРАВИЛА БЕЗОПАСНОСТИ Как и в случае с пранкингом (см. Пранк), главная цель тролля – заставить другого человека «играть по его правилам». По сути, Интернет-тролль – это тот же пранкер. Поэтому воспользуйтесь той же тактикой, не ввязывайтесь в спор с «троллем», не замечайте его. Этому человеку важна прежде всего Ваша реакция - и расстроив вас или разозлив, он почувствует собственное превосходство. Так зачем Вам «кормить тролля»? В крайнем случае, если подобные атаки не прекращаются или задевают уже и Ваших знакомых, друзей – обязательно сообщите администрации сайта или модератору.

Самому троллем быть вообще не рекомендуется – легко потерять друзей в Интернете. А то и вообще могут наказать в реальной жизни, в том числе даже полиция.

ФЛЕШМОБ в Интернете (по-английски flash mob, от слов flash — вспышка, миг, мгновение; mob — толпа; переводится как «вспышка толпы» или как «мгновенная толпа») – спланированная массовая акция в Сети. Понятие «флешмоб» появилось тогда, когда в реальности случайные зрители начали обращать внимание на то, что в общественных местах внезапно собирается группа людей, совершают на первый взгляд бессмысленные действия (например, синхронно танцуют или предлагают обняться совершенно незнакомым людям), а потом так же внезапно расходятся в разные стороны. Однако основой любого флешмоба всегда является четкий сценарий. Два других правила - мнимая спонтанность и случайный набор участников.

Все эти черты перенял виртуальный флешмоб, добавив к чертам оффлайнового флешмоба интерактивность, анонимность и значительное упрощение процесса организации мобберов (участников).

Как правило, целью флешмоба является просто забава. Однако нередко флешмоб может иметь и протестную подоплеку.

ПРАВИЛА БЕЗОПАСНОСТИ В Интернете флешмоб часто используется для какого-нибудь хулиганства – например, коллективно затравить или захамить кого-нибудь на форуме, в социальной сети, по электронной почте. Такой флешмоб – это еще один вид киберунижения. Кстати, через Интернет назначают и управляют и флешмобами в реальной жизни.

ФОТОЖАБА – так называют измененное (переработанное) изображение, картинку, при помощи специальной программы (графического редактора). Одна из самых известных таких программ – Фотошоп (Photoshop) – и породила слово «фотожаба». Его впервые использовал в Сети 19 августа 2004 года одни из пользователей ЖЖ.

Обычно создаваемые изображения носят карикатурный характер, то есть характер насмешки. Так, фотожабы могут базироваться на популярных фотографиях новостей, чаще всего они основаны просто на забавных случайных фотографиях, иногда могут носить идеологическую окраску.

Фотожабой также называют подборку разных тематических картинок, каждая из которых карикатурно изменена. В Сети существуют целые интернет-сообщества, посвящённые фотожабам. Наиболее удачные из них попадают на развлекательные сайты.

ПРАВИЛА БЕЗОПАСНОСТИ «Фотожабы» часто делают для того, чтобы унизить человека или создать ему негативную репутацию. Например, к фотографии «подрисовывают» что-то непристойное, или искажают лицо так, что оно становится неприятным.

Если «фотожабу» про Вас выложили в Сеть – есть смысл обратиться к модератору сайта, где она возникла, или на «Горячую линию» Центра безопасного Интернета в России. Тогда «фотожабу» быстро удалят. Кстати, подросткам постарше нелишне знать: за «фотожабу» можно ответить по закону, что потом очень осложнит будущую жизнь.

ФИШИНГ (по-английски phishing) - так называют интернет-мошенничество. Вообще-то, строго говоря, это всего лишь один из видов жульничества в Сети - когда пользователю подсовывают фальшивые веб-страницы или сообщения от банков или платежных сервисов. Эти страницы или сообщения очень похожи на настоящие – даже могут иметь такой же внешний вид. Но вот расположены они по другому адресу, и деньги, которые переводят через них, попадают прямо к жуликам. Этот вид мошенничества стал так популярен, что часто фишингом называют любое мошенничество в Сети. Словечко «фишинг» - это искаженное английское слово «рыбалка»: дескать, жулики «ловят рыбу» - невнимательных юзеров.

Фишеров очень активно ловят – в первую очередь полиция. Поэтому в среднем одна фишерская страница «живет» очень недолго - два-три дня, а то и вообще полчаса.

ПРАВИЛА БЕЗОПАСНОСТИ Помните, что НИ ОДНА почтовая служба и тем более ни один банк НИКОГДА не запрашивает пароли своих клиентов – ни по почте, ни по Интернету.

Простую фишерскую поделку можно выявить при помощи Интернет-браузера. При наведении мышью на кнопку сайта или ссылку в левом углу браузера обычно проявляется подлинный адрес веб-страницы. Если Вы стали жертвой фишинга, то вместо указанного на странице адреса, например, pay.bank.com в углу проявится какой-то другой, а то и IP-адрес.

Защитные программы довольно неплохо защищают от фишеров – в них есть базы данных таких ресурсов, а еще они умеют анализировать новые страницы. Крупные компании всего мира для борьбы с фишингом создали Антифишинговую рабочую группу – от России в нее входит Лаборатория Касперского.

ХАКЕР (от английского hack — разрубать) - «Интернет-взломщик», тот, кто пишет и использует вредоносные программы против чужих компьютеров. К примеру, хакеры взламывают профили в социальных сетях или «ящики» электронной почты, а так же заимствуют чужие пароли или личную информацию. Делают они это с целью получения выгоды или просто ради забавы. Бывает и так, что хакеры просто атакуют компьютеры вредоносными программами, чтобы вывести их из строя. Для большинства интернет-пользователей угрозы со стороны хакеров ограничиваются именно этими сферами.

ПРАВИЛА БЕЗОПАСНОСТИ Хакеры опасны не только для отдельных пользователей или групп людей, но и для целых коммерческих организаций, крупных информационных ресурсов, государственных систем. Один хакер, попав в секретные

компьютерные системы другого государства, легко заменит Штирлица или Джеймса Бонда. А если хакер украл коммерческую информацию, то убытки от причиненного вреда могут исчисляться миллионами долларов.

За подозрительными атаками обычно следят защитные программы. Так что лучше про них не забывать.

Ч ***«ЦИФРОВОЙ НАРКОТИК»*** – это собирательное название для звуковых файлов, которые будто бы оказывают особое действие на слушателя. Их распространители утверждают, что прослушивание этих файлов способно вызвать такие же эффекты, как от приема настоящих наркотиков, так как там якобы есть специальные «волны».

Однако медики давно доказали, что «цифровые наркотики» - это миф, то есть прослушивание такой музыки не имеет ничего общего с наркотическим эффектом. Она может быть «экзотической» или «тяжелой», но это всего лишь обычная музыка. И действует на мозги не лучше и не хуже, чем любая другая похожая музыка. А те немногие, кто говорит, что «они действуют», в реальности просто убедили себя в том, что они чувствуют «опьянение» - в науке это называется «эффектом плацебо».

ПРАВИЛА БЕЗОПАСНОСТИ Сейчас продажей «цифровых наркотиков» занимаются только мошенники. Они хотят продать обычную музыку за большие деньги как «необычную», называя ее по имени реальных наркотиков. Например, жулики предлагают скачать любой из «цифровых наркотиков на выбор»: экстази, марихуану, ЛСД, викодин и многое другое. При этом за каждый файл необходимо отправить «недорогую» смс, реальная стоимость которой может достигать тысячи рублей. Доверчивому пользователю пишут на сайте стоимость СМС-ки из расчета за один день, в то время как деньги с телефона списываются сразу за 3 месяца доступа.

Ч ***ЧАТ*** — (от английского to chat – болтать) – место, где можно публично общаться в Сети «в режиме реального времени» (то есть как на улице). Участники чата обычно пользуются никами (от англ. nickname) – выдуманными именами, с помощью которого пользователь обозначает себя в Сети. Также чатом можно назвать общение по Skype , так как и там можно обмениваться мгновенными сообщениями в реальном времени. Отличие лишь в том, что Skype дает возможность не только читать сообщения, но и слышать, а также наблюдать за собеседником с помощью видеокамеры. Чаты, где можно слышать и видеть собеседников, называются видеочатами.

ПРАВИЛА БЕЗОПАСНОСТИ Не забывайте, что в чате нужно общаться так же, как на улице – то есть вежливо и с соблюдением правил. Например, не нужно хамить или писать только заглавными буквами (это считается «криком»). Ни в коем случае не принимайте сомнительные файлы от незнакомых людей и не запускайте их у себя на компьютере. И, само собой, не копируйте переписку в чате без ведома собеседника, особенно если чат приватный (то есть предназначен для общения ограниченной группы людей, знающих друг друга).

ШПИОНСКОЕ ПО – Spyware (от английских слов Spy — шпион и Software — программное обеспечение) – это установленная без ведома или против воли пользователя программа, которая скрыто отслеживает поведение пользователя в Сети. Такие программы используются для сбора различных типов личной информации: частота пользования Интернетом и посещаемые сайты (Tracking Software), контроль нажатий клавиш на клавиатуре компьютера (Keyloggers - кейлоггеры), контроль скриншотов экрана монитора компьютера, то есть того, что Вы видите на своем экране (Screen Scraper - скринскреперы). Бывает шпионское ПО и поопаснее – такие программы осуществляют удалённый контроль и управление компьютерами (Remote Control Software), а также незаконный анализ состояния систем безопасности компьютера (Security Analysis Software). Spyware могут менять установки в компьютере для внесения изменений в операционную систему.

Некоторые типы Spyware отключают брандмауэр и антивирусные программы и/или понижают установки безопасности браузера, таким образом, делая систему открытой для другого вредоносного ПО.

Программы-шпионы проникают на компьютер пользователя:

- в комплекте с другими программами;
- с бесплатными пробными (trial) версиями программ;
- вместе со скачиваемыми продуктами;
- посредством обмана пользователя или через уязвимости системы.

ПРАВИЛА БЕЗОПАСНОСТИ Как защитить компьютер от шпионского ПО?

Ознакомьтесь с правилами безопасного серфинга (то есть «путешествия по Интернету») и информацией о новых угрозах.

Запустите антишпионские и антивирусные программы для очистки компьютера.

Убедитесь, что на Ваш браузер и операционную систему установлены последние обновления.

Включите автоматическое обновление программного обеспечения.

Установите в браузере высокий уровень безопасности и конфиденциальности информации.

Игнорируйте всплывающие рекламные окна – то есть не нажимайте на них и не обращайте на них внимания.

ЭКСТРЕМИЗМ – в современной практике под этим термином обычно понимается набор идей, проповедующих ненависть и вражду. Как правило, речь идет о вражде по признаку расы, национальности или принадлежности к религии, причем принадлежность к некоей расе, нации или религии сама по себе является фактором, стимулирующим агрессию. Зачастую экстремисты очень часто призывают к насилию в отношении своих врагов.

Легкость публикации информации в Интернете, его трансграничность и относительная анонимность привлекли в Сеть экстремистов примерно так же, как педофилов. На своих сайтах, на форумах и в социальных сетях они продвигают

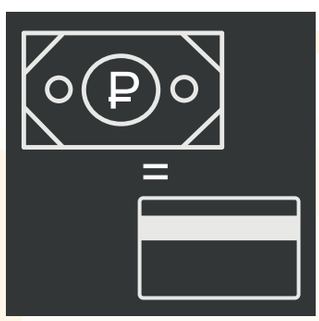
свои взгляды, ищут новых сторонников, очень умело их убеждая (как правило, манипулируя информацией и фактами, смешивая поток проверяемой информации с откровенной ложью, подменяя причины или выводы). Через Интернет они информируют общество о своих действиях, а нередко и планируют их – собирая через Интернет много участников.

Международное право имеет исчерпывающее определение экстремизма – под ним понимается исключительно действие, прямо провоцирующее к вражде или насилию по признаку расы, национальности или религии. Сюда же международное право частично относит пропаганду агрессивной войны. Что же касается критики политического устройства или должностных лиц, которую в отдельных странах (включая Россию) также нередко пытаются включать в понятие экстремизма, то она защищена нормами о свободе слова и, согласно решению Европейского суда, может носить даже «шокирующий» характер.

ПРАВИЛА БЕЗОПАСНОСТИ Зачастую экстремистская идеология препятствует критическому анализу реальности. Человек начинает однобоко воспринимать мир, не может объективно и независимо принимать и оценивать вещи. Бывает и так, что объект экстремистской пропаганды начинает считать, что в его проблемах виноват кто угодно, только не он сам – и перестает работать над собой, профессионально или морально деградируя и ожидая повышение своей востребованности через устранение «конкурентов» другой нации, расы или религии. Чаще же всего «экстремизм» скатывается в обычное хулиганство, от которого страдают люди – часто вообще не имеющие отношения к «проблемам мира», которыми озабочены экстремисты. Кстати, очень часто экстремисты мстят тем, кто раньше разделял их идеи, но вдруг стал сомневаться.

Нередко экстремистская пропаганда рассчитана на подростков и молодежь. В этой связи ребенку лучше порекомендовать на Интернет-сайты с экстремистскими идеями не заходить, а зайдя – тут же выйти. Ничего полезного там не скажут, а вот вреда для дальнейшего развития будет много. Если Вы считаете, что найденное сообщество или сайт опасны для других людей, можно сообщить о нем хостинг-провайдеру или на «Горячую линию».

ЭЛЕКТРОННЫЕ ДЕНЬГИ – специальные денежные единицы, которые используют для совершения покупок и других денежных расчетов в сети Интернет. Хотя они и «электронные», на самом деле это совершенно реальные деньги – те же, что лежат в кошельке или на банковской карте. Ими можно расплатиться там, где эти деньги принимаются – от Интернет-магазинов до онлайн-игр.



Как и в банке, для электронных денег нужен свой личный счет, куда эти деньги можно класть. Счет защищен логином и паролем, а платежи проводятся по так называемому «безопасному соединению». Свой счет можно пополнить покупкой специальной карточки за обычные деньги или в Интернете с банковской карты. А вот перевести электронные деньги в обычные гораздо сложнее и не всегда можно.

Существуют разные системы электронных денег, и обычно с электронного кошелька (счета) в одной системе нельзя расплатиться в другой системе.

ПРАВИЛА БЕЗОПАСНОСТИ Поскольку электронные деньги – это, по сути, самые обычные деньги, то преступники за ними охотятся, как за обычными деньгами. Поэтому нужно внимательно смотреть, сколько и за что Вы платите, и не совершать покупок на подозрительных сайтах. Поскольку в онлайн-играх и в социальных сетях многие дополнительные функции приобретаются как раз за такую «электронную валюту», она становится исключительно популярной среди несовершеннолетних. В этой связи правила обращения с деньгами должны быть распространены для детей и на «электронные кошельки». В частности, ребенок должен усвоить, что нельзя обманом входить в родительские кошельки и платить с них – это все равно, что стянуть у родителей обычный кошелек. Ну и, разумеется, необходимо помнить, что надо хранить свои логин и пароль от электронного кошелька в тайне и никому их не сообщать.

ЭПИК ФЕЙЛ (от англ. FAIL «неудача», «провал», EPIC – легендарный, полный) — означает «претерпевать полную неудачу, иметь сокрушительный провал». Сленговое интернет-словечко из виртуального общения, которое перебралось в реальный мир. Обычно его используют для описания неожиданного и неприятного события, когда человек совершает глупость, «попадает впросак».

Ю

ЮЗЕР (по-английски user) - пользователь Сети. Это слово, как и многие другие, пришло из английского языка, который считается «родным» языком Интернета.

От этого слова образовались производные слова, которые стали так же популярны у рунетчиков:

- Юзать - пользоваться, использовать.
- Юзверь - ничего не понимающий пользователь.
- Юзерпик – то же, что и аватар.

Детям можно предложить следующую памятку для начинающих юзеров - как обеспечить свою безопасность в Интернете.

Не засиживайся долго в Сети. Если тебе только 10 лет, то достаточно и 30 минут. Придумай вместе со взрослыми список домашних правил использования Интернета.

Будь внимателен: в Интернете ты можешь столкнуться с вредной для тебя информацией, злоумышленниками и мошенниками. Если ты столкнулся с чем-то таким, обязательно посоветуйся со взрослыми: проблема может оказаться серьезнее, чем ты думаешь.

Не рассказывай о своей семье. Не делись проблемами с незнакомыми людьми, не сообщай свой адрес.

У тебя появились новые виртуальные друзья? Расскажи о них взрослым. Ведь виртуальный «друг» может оказаться вовсе не тем, кем он представляется в Сети. И взрослые со своим жизненным опытом смогут вовремя заметить опасность для тебя.

Не отвечай на мгновенные сообщения или письма по электронной почте, поступившие от незнакомцев. Если тебя что-то пугает, настораживает или кто-то угрожает в переписке, в письме, обязательно сообщи об этом взрослым.

Попроси взрослых поставить фильтр на компьютер, он защитит тебя от нежелательного материала в Интернете. Пользуйся каталогом детских интернет-ресурсов.

Если ты будешь выполнять эти элементарные правила, то в виртуальном мире тебе будет спокойно, комфортно и интересно.

Я

ЯЩИК – так по-русски называют аккаунт электронной почты. Называют его так по аналогии с почтовым ящиком в «реальном мире». Хотя сейчас «аккаунт» и «ящик» для многих – одно и то же, строго говоря, разница между ними все-таки есть. Для специалистов аккаунт – это учетная запись (логин и пароль), а ящик – входящие и исходящие письма.

Как защитить свой ящик электронной почты – можно посмотреть в статье «E-mail».

НЕ ДОПУСТИ!

РОЦИТ

СОПРОТИВЛЕНИЕ
правозащитное движение

ОБЩЕСТВЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ
CIVIC CHAMBER OF THE RUSSIAN FEDERATION

Уполномоченный при Президенте Российской Федерации по правам ребенка

INTERNATIONAL ASSOCIATION OF INTERNET HOTLINES
INHOPE
ins@fe

Co-funded by the EU under Safer Internet Programme

International Centre
FOR MISSING & EXPLOITED CHILDREN

KASPERSKY lab

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента РФ № 115-рп от 29.03.2013 г.

Safer Internet Centre is co-funded by the EU under Safer Internet Programme