АЗБУКА ИНТЕРНЕТ-БЕЗОПАСНОСТИ

ЦЕНТР БЕЗОПАСНОГО ИНТЕРНЕТА В РОССИИ

РОЦИТ

KASPERSKY lab

Дорогие друзья!

Интернет - это огромный мир, который окружает нас все то время, что мы проводим за компьютером. Однако он влияет на нас и тогда, когда мы за компьютером не сидим. Потому что Интернет – это не отдельный мир, а часть нашей обычной жизни.

Эта часть может быть увлекательной, а может быть и опасной. И какая она будет, зависит во многом от нас самих. От того, насколько много мы знаем об Интернете. О тех вещах и программах, что там есть, и о том, как их правильно использовать. О том, как вести себя в Сети. И, конечно же, о том, как некое действие в Сети может отразиться на повседневной жизни кого-то вокруг – а может, и на нас самих.

Наша «Азбука» рассказывает об основных понятиях, сервисах (службах) и вещах в Интернете – и о том, как они влияют на нашу безопасность. Причем не только на безопасности в Сети, но и в обычной жизни. Из «Азбуки» можно узнать о том, как Интернет-угроза может прийти из обычного сайта или программы – и о том, какие меры нужно принять, чтобы защититься от разных Интернет-угроз.

Всемирная Паутина – так еще называют Интернет – становится все нужнее и нужнее любому современному человеку. При этом соблюдение правил безопасности в Сети может уберечь от большой беды в обычной жизни. Надеемся, что наша краткая Азбука поможет вам уверенно войти в мир безопасного, а значит – интересного и удобного Интернета.

Успехов вам!

Создатели «Азбуки Интернет-безопасности».

А

Аватар (*он же аватара, он же аватарка, он же ава, он же юзерпик – от английского user picture — картинка пользователя*) — **это фотография или картинка, представляющая пользователя в виртуальных просторах. Проще говоря, это ваше «лицо» в Сети.** Аватары используются на форумах, в чатах, блогах, социальных сетях, различных играх.

Считают, что происхождение этого термина нужно искать в философии. На русский язык «аватар» обычно переводится как *«воплощение»* - кого-либо в ином образе.

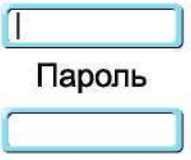
Аватаром может быть реальная фотография человека или какая-то картинка. В этом ему помогает никнейм (он же «ник»), которым пользователь называет себя в Сети. Он тоже может быть выдуманным или реальным именем. Аватары обычно иногда меняются.

Правила безопасности:

Будьте разборчивы, не забывайте, что мнение о вас в Сети сложится в первую очередь по тому, что увидят другие пользователи. Вспомните русскую поговорку «Встречают по одежке, а провожают по уму».

Не следует ставить слишком откровенные фотографии на заставку, это может привлечь Интернет-хищников и хулиганов. Такие фотографии могут увидеть и ваши учителя, соседи или просто знакомые. Так же не ставьте на аватар фотографии, по которым можно судить о материальном благополучии вашей семьи. Нехорошо также ставить на аватарку фотографии других людей.

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 некие 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 (то есть строго личной) информацией и не должны быть видны другим пользователям – за исключением того, что вы сами разрешите им видеть о себе. Вещи, 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 или установить новый пароль за вас он не может.

Правила безопасности:

Запомните, что никогда администратор или модератор сайта 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!

Бан (*от английского ban — запрещать, объявлять вне закона*) - **наиболее действенная форма наказания Интернет-хулиганов и контроля за их поведением.** Обычно это означает лишение нерадивого 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 тут не поможет.

Бан накладывается администратором или модератором сайта. На некоторых сайтах бан можно обжаловать у совета модераторов.

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.

Баннер (*от английского banner — флаг, транспарант*) – **«интернет-плакат»**. Иногда меняющийся, как мультфильм (то есть «анимированный»), иногда обычная картинка. Баннер стал основной формой интернет-рекламы. Баннер может быть и озвучен – то есть к нему может быть привязана музыка или речь.

Правила безопасности:

Главная ценность многих баннеров - ссылка, по которой – нажав на баннер – можно попасть на другой сайт. Обычно это сайт, который этот баннер рекламирует. Но бывает и так, что человек попадает на сайты мошенников, хулиганов 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. А еще часто бывает, что внизу страницы отображается ссылка, на которую ведет баннер – внимательно смотрите, куда она ведет.

Браузер (*по-английски browser – «просматриватель»*) – **та самая программа, в которой открывают и смотрят веб-сайты.** Слово тоже английское и буквально значит «просматриватель». 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. Это 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 на зараженный сайт и атака будет незаметно произведена. Поэтому вы должны быть бдительны и не попадаться на уловки мошенников – например, на такие сообщения: «Ваш компьютер инфицирован; загрузите эту антивирусную программу». Спросите свой антивирус – он точно скажет, заражен ваш компьютер или нет.

Вирус – вредоносная программа, созданная специально для стирания, блокирования, изменения или копирования информации на компьютере – против воли его хозяина. Вирусы могут нарушать работу компьютеров или целых компьютерных сетей.

Вирусы попадают на компьютер различными способами: либо человек сам по своей доверчивости и наивности запускает на своей машине вредоносную программу, либо злоумышленники рассылают ее под видом безобидных приложений или игр. Учтите, антивирус не всегда может предотвратить заражение компьютера.

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» (это еще один вид опасных программ) могут саморазмножаться в компьютерах и компьютерных сетях, почти все они распространяется 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. Название идет от известного греческого произведения «Илиада», где греческие воины спрятались в деревянном «троянском коне» и обманом попали внутрь осажденной ими Трои. Изначально в «трояне» не заложено

вредительских функций, но хозяин вредоносного кода, пользуясь чужим компьютером, может украсть личную информацию жертвы, завладеть её паролями и сделать многое другое.

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 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 жертве многочисленных запросов через Интернет. Компьютер не может с ними справиться и «зависает». Если это сервер, то станут недоступны привязанные к нему Интернет-сайты. Зараженные вредоносной утилитой компьютеры 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).

Как защититься?

- Установите антивирус;
- Регулярно следите за его обновлением и скачивайте новые антивирусные базы.
- Будьте внимательны при работе в Интернете: не переходите по неизвестным ссылкам и не скачивайте подозрительные файлы.

! Не верьте «халяве», когда вам обещают вскрыть страницу интересующего вас пользователя или открыть еще какие-либо тайны, а для этого надо лишь пройти по ссылке.

! Если заражение уже произошло, отключите компьютер от Сети. Если в Сети есть еще компьютеры, смените все пароли.

! Если вам не удается избавиться от вредоносного кода самостоятельно – обратитесь к специалисту, но ни в коем случае не платите вымогателям и не отправляйте смс-сообщения на короткие номера.

Г

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 профессионалы, 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 вирутальный 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.

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 об опасном контенте или опасных действиях в Сети.** Сообщить о плохом сайте можно анонимно – то есть никто не будет знать, кто именно отправил сообщение. Отправить сообщение очень просто – надо скопировать из браузера и вставить в окно «Горячей линии» ссылку на плохой сайт, и еще указать, к какой категории этот сайт по-вашему относится.

Все сообщения на «Горячую линию» обязательно проверяются опытными аналитиками – специалистами по контенту в Интернете. Они могут профессионально определить, опасный этот контент или нет. Если контент опасен, то «Горячая линия» сообщит провайдеру, и тот немедленно закроет контент. А если надо, о плохом сайте или Интернет-хищнике узнают и правоохранительные органы – они найдут злоумышленника и привлекут к ответу по закону.

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. То есть, если злоумышленник спрятал свой сайт в другой стране или спрятался там сам, то это ему не поможет.

Если вы встретились с опасным контентом – обязательно сообщите о нем на «Горячую линию» Центра безопасного Интернета! Этим вы защитите и себя, и других пользователей Сети.

Груминг *(от английского grooming)* – **так называют действия интернет-хищников по поиску и завлечению своих жертв через Интернет.** Интернет-хищник знакомится с ребенком в социальной сети, в чате, на форуме, через электронную почту. Он может представляться как взрослым, так и ребенком. После чего он начинает всячески втираться в доверие к ребенку и подростку.

Завоевав доверие, он начинает побуждать ребенка совершать нехорошие вещи – например, переслать ему свои фото в неприличном виде. Главная цель груминга – добиться реальной встречи с ребенком, чтобы его похитить и сделать очень больно.

Правила безопасности:

Нужно всегда помнить, что виртуальный друг должен оставаться виртуальным! В Сети можно представиться кем угодно: хоть бабушкой, хоть известным киноактером, хоть «черепашкой-ниндзя». Поэтому на реальные встречи с Интернет-друзьями надо обязательно ходить с родителями.

Если виртуальный «друг» начинает вести себя непристойно – например, побуждать к непристойным действиям, пересылать посты и фото непристойного вида, заводить беседы на непристойные темы – надо ОБЯЗАТЕЛЬНО прервать общение с таким «другом» и рассказать о нем родителям. Такой «виртуальный друг» может принести ОЧЕНЬ много вреда и тебе и другим сверстникам!

Гуглбомбинг (*по-английски Googlebombing, также используется термин link bomb – «бомбежка ссылками»*) - **специальная хакерская шутка. 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 сотворить подобную «шутку», хакеры пользуются специальными компьютерными программами, которые оценивают Интернет-страницы. А оценивают они 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.

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 (то есть неповторимая).

Д

Домен – (*от английского domain – область, поле деятельности*). **Это то, что мы привыкли считать адресом сайта.** Вообще-то, строго говоря, домен - это буквенное обозначение адреса сайта, более привычное и удобное по сравнению с IP-адресом (который в цифрах). Пример: IP-адрес - 123.456.78.90 или доменное имя adres.com. Что удобнее? Кроме того, доменное имя сайта способно сразу сообщить о нем много интересной информации. Так 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).

Правила безопасности:

При посещении неизвестного вам сайта обращайте особенное внимание на его правильное написание. 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.

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.

Е

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@saferunet.ru значит, что адрес info привязан к почтовой системе сайта saferunet.ru.

Правила безопасности:

Мошенники очень часто используют для спамерских атак и рассылки вирусов именно электронную почту. Поэтому старайтесь не оставлять свой адрес на всех сайтах 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!

ЖЖ, ЖэЖэ, Жежешечка – **популярный сервис блогов LiveJournal** (*«Живой Журнал»*). Блог - (*по англ. blog, от web log — интернет-журнал событий*) - это интернет-дневник, только не в школьном, а в личном смысле. Такая личная интернет-газета, которую может выпускать каждый – и при этом общаться с читателями. Отличие блога от страницы в социальной сети или персонального сайта

Ж

состоит в том, что главное в блоге – это твои тексты. Размещаются они обычно так: 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).

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.

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, который выкладывают в Сеть.

З

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».

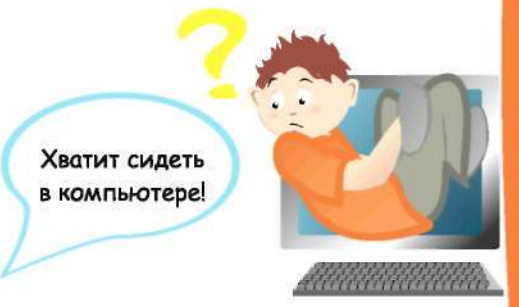
Интернет-зависимость (*по-английски Internet addiction*) – **состояние, когда человек чувствует сильное желание как можно больше времени проводить в Интернете и очень болезненно переживает моменты, когда не может туда попасть.** Бывает, что интернет-зависимые люди сидят в сети сутками и даже умирают от этого.

И

Некоторые врачи считают, что Интернет-зависимость – это такое 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 деньги или порносайтам.

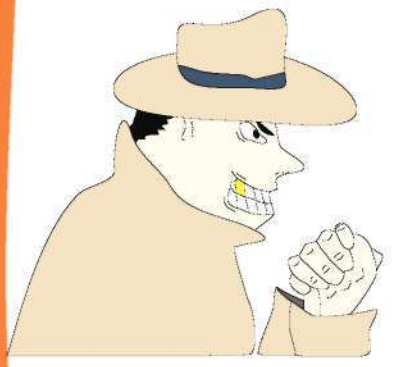


Правила безопасности:

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.

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.

Интернет-хищник *(от английского Internet-predator)* – взрослый человек, который хочет делать плохие или неприличные вещи с детьми и подростками. Поскольку в реальной жизни его за это могут легко побить или посадить в тюрьму, «хищники» стремятся искать своих жертв в Интернете. И, надо сказать, они делают это очень изобретательно – выдают себя за таких же детей и подростков, известных певцов и актеров, благотворителей и так далее. Своих жертв «хищники» ищут в социальных сетях, на форумах, в чатах, могут познакомиться даже по электронной почте. Как они это делают, можно прочитать в статье «Груминг».



Название «Интернет-хищники» появилось в Америке. Самоназвание «интернет-хищник» переводится с греческого как «тот, кто любит детей». Но их «любовь» полностью ломает жизнь детям и подросткам.

Правила безопасности:

Если возникло ощущение, что «виртуальный друг» - интернет-хищник, то надо немедленно сообщить родителям, учителю или на «Горячую линию». «Хищник» может быть очень жесток – и всегда опасен! Однако не надо рассказывать всем о своем контакте с ним – все могут понимать это по-разному.

Контент (*по-английски content - содержимое*) - **то, что находится на сайте.** А точнее - информация или материалы, которые пользователь может прочитать, посмотреть, послушать или скачать с этого сайта. Например, контент шкафа - одежда, контент холодильника - еда.

Основные виды контента: текст; графика (картинки, изображения); медиаконтент (видео- и аудиофайлы).

Контент делится на позитивный и негативный, то есть «хороший» и «плохой». Негативный контент несет угрозу не только работе компьютера, но и самому человеку. Вместе с вирусами и действиями Интернет-мошенников такой контент называют «Интернет-угрозы». Их великое множество в Интернете, поэтому лучше на такие сайты не попадать и не заходить. Прочитай Азбуку от А до Я и тебе проще будет обезопасить себя. Позитивный контент - это интересные, полезные и хорошие сайты. Они помогают учиться, получать новые и интересные знания, развлекаться и общаться в безопасной среде. Часто такие сайты объединены в «белые списки», по которым работают защитные программы. В России эти программы предлагают фирмы-операторы «проводного» и мобильного Интернета. А среди сайтов с «хорошим» контентом регулярно проводятся конкурсы.

Правила безопасности:

Весь контент в Интернете охраняется законом об авторских правах и всегда имеет авторов и владельцев. За незаконное скачивание или «заимствование» из Интернета могут привлечь к ответственности.

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.

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).

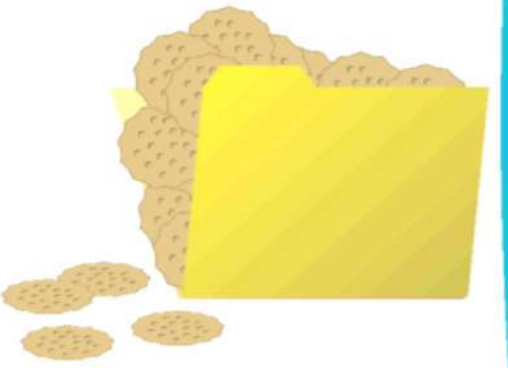
Практически на всех форумах и сайтах, где есть возможность общаться, существует функция, позволяющая заблокировать «нехорошего» пользователя. В крайнем случае, не так трудно удалить свою анкету с сайта знакомств или из социальной сети, чтобы не быть больше мишенью для оскорблений и травли. Кроме того, 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 (например, http://www.saferunet.ru/).

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. 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».

Л

«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 через сайт Центра безопасного Интернета **saferunet.ru**, а если нужна помощь психологов – через специальный сайт **psyhelpline.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 и используют 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. Он наделен особыми правами по сравнению с остальными – может править чужие посты, выносить предупреждения или банить Интернет-хулиганов. Денег он обычно за это не получает. На каждом форуме или сообществе существуют правила, за соблюдением которых и следит модератор.

М

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 – тогда лучше просто уйти с такого сайта. Потому что похожих сайтов много, а модераторы на других сайтах могут быть лучше.

Неприличный контент - **фотографии, видеоролики или тексты, где дети и подростки совершают непристойные действия, очень часто со взрослыми.** Зачастую для этого детей обманывают или запугивают.

Н

Неприличный контент очень унизителен для ребенка, который там изображен. Те, кто его видели, и узнали показанного там человека, могут над ней смеяться или издеваться – от этого ему становится еще хуже. Поскольку Интернет всемирный, то неприличный контент, выложенный в одной стране, могут посмотреть в любой точке земного шара. Обычно неприличный контент делают и распространяют Интернет-хищники.

Правила безопасности:

Если вам встретились сцены с неприличным контентом в Сети – немедленно примите меры! Сообщите о нем на «Горячую линию» и в полицию.

Неприличный контент обычно появляется так: «хищник» просит ребенка сделать непристойные действия через веб-камеру своего компьютера, записывает видео и выкладывает через Интернет. Поэтому, если ваш виртуальный собеседник просит сделать что-то неприличное перед компьютером или камерой (например, раздеться) – этого делать ни в коем случае нельзя! А о такой «просьбе» лучше сразу рассказать родителям.

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. 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 на веб-форуме, 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.

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

П

Провайдеры бывают разные:

Хостинг-провайдер – это тот, кто разрешает размещать на своих серверах сайты и у кого эти сайты хранятся. Нередко 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 позволяет нам соединяться с Интернетом через провода или мобильники.

http://

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. Пранк-культура, равно как и сам термин «пранк», появились в России на рубеже XX—XXI веков.

Правила безопасности:

Пранк – это не шалость, а преступление, и за него можно ответить по закону. Никогда не занимайтесь «телефонным хулиганством» и не выкладывайте такие записи в Интернет!

Если вы 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 не гранатомет, а компьютерная ролевая игра.** В ней пользователь играет от имени одного героя или группы героев. Как правило, суть игры состоит в том, что выполняя квесты (задания, которые по сюжетной линии даются основными или дополнительными игровыми

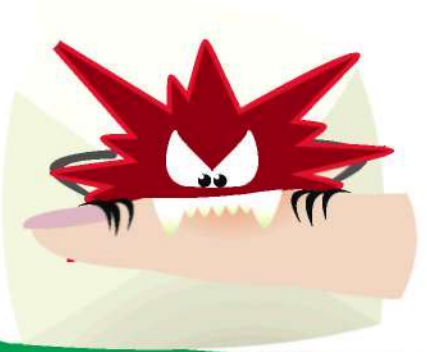
персонажами), герой повышает свой уровень и имеет возможность развивать свои характеристики, улучшать броню и оружие и так далее. Обычно в этом случае пользователь играет напрямую «с компьютером».

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 не забывайте простые правила безопасности: соблюдать законы поведения, не грубить, не мешать играть другому человеку, не нарушать законы игрового мира.

Спам (*сокращение от англ. «spiced ham» - ветчина со специями*). **Интернет-пользователям это слово хорошо знакомо как обозначение сообщений, 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.



С

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.

Обязательно нужно 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 непристойного 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, дети рано или поздно

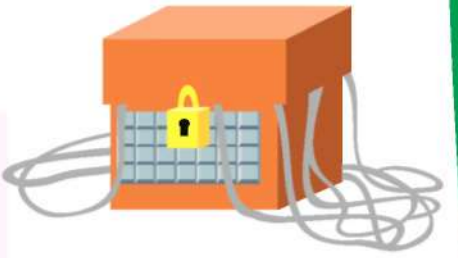
замечают, что самой большой популярностью пользуются те из них, где они сняты полуобнажёнными.

Правила 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 вас 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 вы, сами того не осознавая, можете спровоцировать Интернет-хищников на преступные действия.

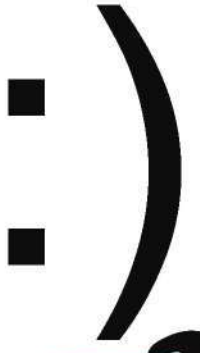
Сервер – большой компьютер, при помощи которого «раздают» Интернет или на котором хранится информация в Интернете.



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:

:-)	;-)	:-O	:(	:`-(
Улыбаюсь	**Подмигиваю**	**Удивляюсь**	**Грущу**	**Плачу**

:-P	:-D	:-*	}:-)	^_^
Показываю язык	**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 таковы:

- Подумай, прежде чем что-то написать или опубликовать в Интернете. Ты можешь подсказать хулиганам и преступникам, как лучше тебе причинить вред.
- Не выкладывай в социальной сети личную информацию и тем более личные фотографии. Помни: все, что ты выложил в сети, увидят другие. А что они с этим сделают – вопрос...
- Не «френди» всех подряд. Дружи в социальных сетях 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 не публикуй в социальной сети то, что может обидеть и унизить других пользователей или просто других людей! Даже в шутку – такие «шутки» плохо кончаются.
- Проверяй антивирусом все присылаемые «приложения».
- Никогда не играй в социальной сети на деньги и не запускай приложения, требующие денег за участие или поднятие в них своего «статуса».
- Если ты стал жертвой оскорблений или опасного контента – сообщи администратору социальной сети или на «Горячую линию».

Торрент – (*по-английски torrent – поток*) - **обширнейший** (то есть очень большой) **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 часто 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. В общем, троллей в Интернете не любят. Тролли получают удовольствие от негативной (то есть плохой, резкой) реакции других людей. Поэтому они намеренно идут на ссору 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, что и раньше – не ввязывайтесь в спор с «троллем», игнорируйте 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.

Ф

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 ним интерактивность, анонимность и значительно упростив процесс организации мобберов (участников).

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 один 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 плохую славу. 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 надо 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 атакуют компьютеры вредоносными программами, чтобы вывести их из строя. Для большинства интернет-пользователей угрозы со стороны хакеров ограничиваются именно этими сферами.

Х

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.

«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».

Ц

Впрочем, медики давно доказали, что «цифровые наркотики» - это миф. То есть такая музыка не имеет ничего общего с наркотиками. 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. 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 у себя на компьютере. И, само собой, не копируйте переписку в чате без ведома собеседника, особенно если чат приватный.

Ш

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 умеют делать удалённый контроль и управление компьютерами (Remote Control Software), 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 неприкрытой 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 – **набор идей, проповедующих ненависть и вражду.** Некоторые люди очень легко обвиняют во всех проблемах людей другого цвета кожи, национальности или религии – считая, что они повинны во всех проблемах только потому, что они родились на свет. При этом экстремисты очень часто призывают к насилию в отношении этих людей – призывают их бить, убивать, выгонять.

Поскольку в Интернете очень легко опубликовать информацию, экстремисты очень «полюбили» Интернет. На своих сайтах, на форумах и в социальных сетях они продвигают свои взгляды, ищут новых сторонников, очень умело их убеждая – в Интернете лгать легко. Через Интернет они рассказывают о своих действиях, а нередко и планируют их – собирая через Интернет много участников.

Важно отметить, что люди, которым не нравятся правители или политическая ситуация, экстремистами не являются – если, конечно, они не призывают свергать власть. Так говорят международные законы.

Правила безопасности:

Идеи экстремистов ни к чему хорошему не приводят. Человек начинает однобоко воспринимать мир, не может объективно (то есть независимо) принимать и оценивать вещи. Он начинает считать, что в его проблемах виноват кто угодно, только не он сам – и перестает работать над собой. В результате он не может стать хорошим профессионалом, работником, специалистом. А чаще 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.

Лучше всего 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 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. Само собой, нельзя обманом входить в родительские кошельки и платить с них – это все равно, что стянуть у родителей обычный кошелек. Ну и, разумеется, 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».

Юзер (*по-английски user*) - **пользователь Сети**. Это слово, как и многие другие, пришло из английского языка, «родного» языка Интернета.

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

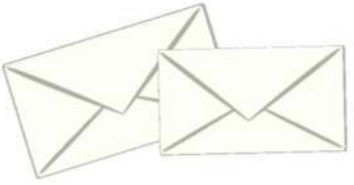
Юзать - пользоваться, использовать.

Юзверь - ничего не понимающий пользователь.

Юзерпик – то же, что и аватар.

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 – смотри в статье «**E-mail**».



Памятка 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.

ОСНОВНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ ОТ ЛАБОРАТОРИИ КАСПЕРСКОГО

(для родителей)

Объясните детям несколько простых правил — будет намного лучше, если ребенок узнает правила безопасного поведения в Интернете от родителей, а не из собственного печального опыта. Как говорится, в данном случае «лучше учиться на чужих ошибках».

➔ В Сети нельзя оставлять в открытом доступе (там, где все это могут увидеть) или отправлять незнакомцам по почте, при общении в социальной сети или в чате подробную информацию о себе — сейчас любой злоумышленник может выследить человека по его адресу или номеру телефона.

➔ Не следует доверять ссылкам в письмах и сообщениях от неизвестных вам людей. Это может быть небезопасно, поскольку сообщение может быть отправлено хулиганами или мошенниками.

➔ Кроме того, не надо верить сообщениям, где вам пишут о том, что вы выиграли бесплатный подарок, приз или можете легко заработать деньги, предлагают поднять «рейтинг» или получить «супервозможности» в социальной сети. Скорее всего, все закончится тем, что вас заманят на вредоносную веб-страницу и заразят ваш компьютер вирусом.

➔ В целом, общаться и вести себя в Интернете ребенок должен так же осторожно, как и в реальной жизни.

ЛАБОРАТОРИЯ КАСПЕРСКОГО

Лаборатория Касперского – ведущий российский производитель антивирусного программного обеспечения и комплексных программно-технических защитных продуктов. Компания, основанная в 1997 году, сейчас уверенно входит в четверку мировых лидеров - производителей программных решений для защиты конечных пользователей. Продукты «Лаборатории Касперского» защищают более 300 млн. пользователей по всему миру – причем не только их компьютеры и серверы, но и мобильные телефоны.

«Лаборатория Касперского» - одна из немногих российских инновационных компаний, хорошо известных и популярных на Западе. За время своей работы Лаборатория превратилась в международную группу компаний с представительствами в 29 странах мира. В рекламе Лаборатории Касперского снимаются мировые звезды кино – например, Джеки Чан. Многие технологии, без которых трудно представить себе современный антивирус, впервые были разработаны именно «Лабораторией Касперского» - не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики в разных странах (в том числе в США).

Хотя основная «тема» Лаборатории – защита от зловредов (вредоносного ПО) и Интернет-мошенничества, Лаборатория уделяет серьезное внимание контентным Интернет-угрозам. Компания проводит регулярные исследования подверженности пользователей контентным угрозам и на основе них адаптирует свои программные продукты. В комплексном защитном ПО от Касперского присутствуют функции «родительского контроля» и контентного фильтра, способные защитить ребенка и подростка от негативного контента. В результате пользователю не нужно приобретать отдельно антивирус и отдельно контентный фильтр – все эти функции содержатся уже в одном продукте.

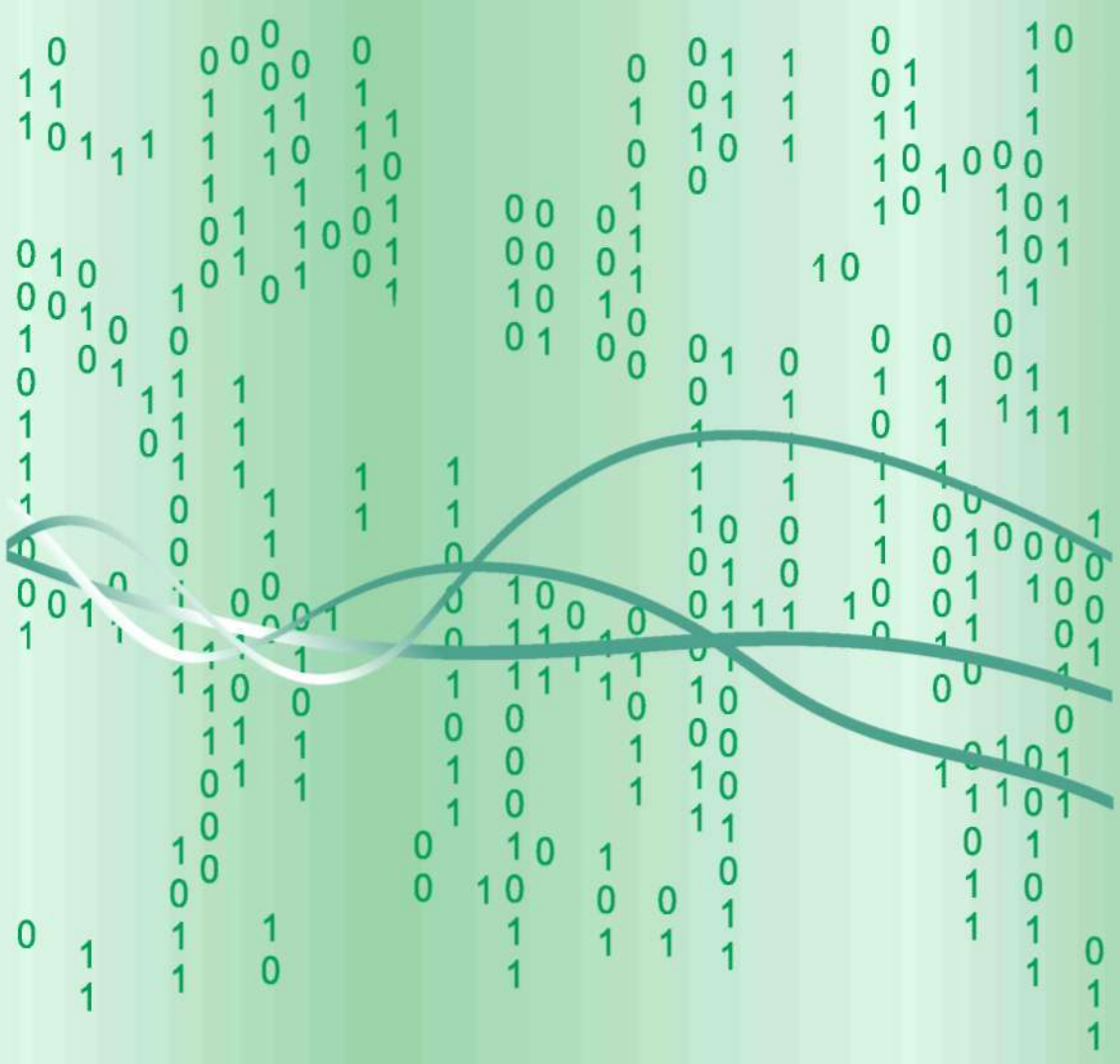
ЦЕНТР БЕЗОПАСНОГО ИНТЕРНЕТА В РОССИИ

Центр безопасного Интернета в России – ведущий российский общественный проект в области формирования безопасного Интернет-пространства для детей, молодежи и взрослых, а также защиты от опасного и противоправного воздействия через Интернет и мобильные технологии. Центр действует с 2008 года, опираясь на сеть региональных представительств. Создатели Центра – РОЦИТ и движение «Сопротивление»; проект действует под патронатом Общественной палаты РФ.

В рамках Центра действуют:

- Информационно-просветительские и специальные проекты (главный из которых – портал Центра **www.saferunet.ru**);
- «Горячая линия» по приему анонимных сообщений о противоправном контенте;
- «Линия помощи» - сервис анонимных консультаций и психологической помощи по вопросам Интернет-опасностей;
- Молодежная Интернет-Палата – сообщество молодых сторонников безопасного Интернета.

Центр безопасного Интернета в России представляет нашу страну в Европейской сети Центров безопасного Интернета Insafe, является членом Международной сети «горячих линий» INHOPE. Центром и его партнерами регулярно проводятся просветительские и образовательные мероприятия по теме безопасности в Сети и повышения своей «сетевой грамотности».



ЦЕНТР БЕЗОПАСНОГО ИНТЕРНЕТА В РОССИИ

РОЦИТ

KASPERSKY lab

saferunet.ru

Центр Безопасного Интернета в России
Общественная Палата Российской Федерации
125047, Москва, Миусская площадь, 7 стр. 1
E-mail: info@saferunet.ru

Концепция и текст: Урван Парфентьев, Кристина Куницына, Мария Епифанова
Рисунки и дизайн: Олеся Тимофеева
Консультант : Марк Твердынин

Все права защищены и являются собственностью Центра Безопасного Интернета в России (РОЦИТ). По всем вопросам просьба обращаться на электронный адрес info@saferunet.ru

(c) РОЦИТ, 2011. Тираж 1000 экз. Распространяется бесплатно. НЕ ДЛЯ ПРОДАЖИ

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента Российской Федерации от 8 мая 2010 года №300-рп
Отпечатано в типографии "РПФ НИК"(г.Москва, Бутырский вал., Приютский переулок, дом 3)