РОЦИТ

БЕЗОПАСНЫЙ ИНТЕРНЕТ

КРАТКИЙ КУРС

ФОНД ИНФОРМАЦИОННОЙ ДЕМОКРАТИИ

РАЭК

При реализации проекта используются средства государственной поддержки, выделенные в качестве гранта в соответствии с распоряжением Президента Российской Федерации от 01.04.2015 № 79-рп и на основании конкурса, проведенного Фондом ИСЭПИ.

ЧТО НАС ПРИВЛЕКАЕТ В ИНТЕРНЕТЕ, И КАКИЕ «ПОДВОДНЫЕ КАМНИ» НАС ТАМ ЖДУТ?

Интернет – кладезь информации, неисчерпаемый источник общения, бездонное море пользовательских приложений и бескрайние просторы для действий различных криминальных и полукриминальных личностей.

Открывая интернет-браузер в предвкушении интересного интернет-серфинга надо не забывать о безопасности, как катаясь на роликах не помешает обзавестись наколенниками и налокотниками.

На полках книжных магазинов сейчас можно найти различные издания на тему безопасности в интернете. Многие из них достаточно объемны и оперируют терминами типа «укажите в firewall исчерпывающий список программ и доступных им портов и сервисов», другими словами они рассчитаны на пользователей, обладающих специализированными знаниями и располагающих лишним свободным временем для того, чтобы все это прочитать. Мы же постараемся, не углубляясь в «технические дебри», дать основные знания по указанной теме.

Итак…

Буклет постарается дать простые, не перегруженные техническими терминами и не требующие углубленных знаний ПК, ответы на вопросы, как обезопасить себя и своих близких при «прогулках» по просторам «глобальной паутины».

СОЦИАЛЬНЫЕ СЕТИ И ФОРУМЫ

Радости онлайн-жизни

Россия сегодня – лидер по времени, проводимому пользователями в соц. сетях. У нас есть «ВКонтакте», «Одноклассники» и импортный «Facebook»… Социальные сети «лишают» нас одиночества и скуки – там всегда есть с кем поговорить, обсудить только что вышедший фильм, похвастаться новым платьишком… Внутри соц. сетей создаются профессиональные сообщества и группы по интересам, где можно узнать «за просто так» то, для чего в обычной жизни надо прочитать немало печатных текстов или прослушать курс лекций в каком-нибудь учебном центре, а иногда и найти настоящих реальных друзей. Форумы – площадки, создаваемые для обсуждения какого-то конкретного вопроса, и являющиеся более узким вариантом социальной сети, – позволяют быстро найти ответы на интересующие вопросы.

НЕПРИЯТНОСТИ

ИСПОЛЬЗОВАНИЕ ЛИЧНЫХ ДАННЫХ

Случай с похищением сына известного российского предпринимателя показал, что бездумное распространение сведений о себе в соц. сетях может дорого обойтись Вам или Вашим родным.

Похищение сына известного российского предпринимателя было совершено весенним утром 2011 года в г. Москва рядом с офисом компании, где он работал программистом.

Двое мужчин затолкали молодого человека в машину и увезли. Через некоторое время преступники потребовали у родителей похищенного €3 млн. за его освобождение. Родители похищенного обратились за помощью в полицию и через несколько дней молодой человек был освобожден в результате спецоперации, а его похитители были задержаны.

Примечательно, что жертву для предстоящего похищения подбирали, руководствуясь списком самых богатых людей России, опубликованным журналом Forbes, а план разрабатывали исходя из информации, которую сын бизнесмена разместил в социальных сетях в интернете. Так, например, молодой человек опрометчиво указал в Сети место своего жительства, учебы и работы с адресами, писал о своем графике и маршруте следования от дома до работы.

Подготовлено по материалам СМИ «CNews.ru»

Конечно возможно Вы не являетесь известным бизнесменом из первой сотни российской элиты, но стать жертвой домушников, которые из поста[1] «ВКонтакте» знают, что с 1 по 15 вы всей семьей будете «греться на солнышке в Египте» вполне возможно.

ОТСЮДА СЛЕДУЕТ ВАЖНОЕ ПРАВИЛО:

- Меньше конкретных данных о своей жизни.
- Не публикуйте информацию, по которой можно определить Ваш домашний адрес и время, когда там никого не бывает.
- Не размещайте в общем доступе посты о дорогостоящих покупках или сделках, в результате которых можно сделать вывод о наличии у Вас крупной суммы денег или ценностей, которые можно перепродать.
- Не описывайте свой постоянный маршрут, пролегающий между домом и работой – нападения с целью ограбления не всегда бывают случайными.
- Если очень хочется поделиться радостью от начинающегося отпуска, добавьте к сообщению приписку о включенной охранной сигнализации (даже если это не правда) – это наверняка отпугнет «продвинутых» любителей легкой наживы.

[1]«Пост» - отдельное сообщение в блоге или форуме.

ТРОЛЛИНГ

Троллинг – агрессивные, оскорбительные или провокационные комментарии в социальных сетях, призванные обидеть или разозлить автора «поста».

«Сделал гадость – сердцу радость» – тролль пишет, следуя именно этой поговорке. В критике тролля чаще всего нет ни грамма конструктива. Именно Ваше раздражение и огорчение доставляют ему наибольшую радость. Целью троллинга зачастую является **привлечение внимания к себе** – тролль хочет почувствовать свою значимость, произвести впечатление, даже если это впечатление резко негативное. Поэтому если на Ваш восторженный «пост» о Вашем родном районе Вы получить комментарий: «В этом районе живут только лохи!», знайте – к Вам в гости пришел тролль.

Не смотря на вроде бы небольшие масштабы проблемы, тролли могут создавать серьезный дискомфорт при общении в социальных сетях.

14-летняя Меган (США) была уверена, что она некрасивая, толстая и никому не нужная. За 5 недель до смерти ее добавил в друзья в социальной сети «MySpace» парень по имени Джош Эванс. После недолгой милой переписки Меган надоела Джошу, он «отфрендил» ее и начал писать ей гадости. Вскоре к развлечению подключились их виртуальные знакомые. Последним сообщением от Джоша, которое прочитала Меган, было: «Мир стал бы лучше без тебя». Она выключила компьютер, и через 20 минут повесилась в гардеробной комнате, где ее и нашла мать.
Через некоторое время родители Меган узнали, что Джоша никогда не существовало. Его страницу, прикола ради, создали три женщины: взрослая соседка семьи Меган, ее дочь и молодая подчиненная.

Подготовлено по материалам интернет-ресурса «Pics.ru»

ЧТО ДЕЛАТЬ, КОГДА ТЕБЯ ТРОЛЛЯТ?

- Спорить с троллем, если ты сам не являешься еще большим троллем, бесполезно.
- Игнорируйте тролля, не отвечайте ему и не пытайтесь доказать, что он не прав. Не поддавайтесь искушению ответить троллю «железными аргументами». Задача тролля не найти истину, а вывести Вас из себя, поэтому большим разочарованием для него будет Ваше молчание в ответ.
- Можно «забанить» тролля – то есть внести его в Ваш личный «черный список». Для этого в некоторых соц. сетях есть специальные кнопочки, в других – необходимо обратиться к модератору[2].

[2] Модератор – пользователь форума или сайта, имеющий право редактировать и удалять сообщения других пользователей и даже удалять или блокировать самих пользователей, нарушающих правила сайта.

Действующий британский боксер Кертис Вудхаус выследил интернет-тролля, который донимал его сообщениями в социальной сети. «Уходи на пенсию немедленно. Не можешь даже защитить свой жалкий титул…», – писал тролль. В ответ на это боксер пообещал тысячу фунтов за адрес и фотографию этого человека. Когда Вудхаусу удалось получить указанную информацию, он опубликовал их в «Твиттере» и пообещал, что «скоро увидится» с интернет-троллем, который получит «хорошую взбучку». По мере продвижения к дому обидчика спортсмен публиковал в соц. сети сообщения о том, что он находится «в 47 минутах», «в 17 милях» и, наконец, «в 10 минутах» от цели. Добравшись до нужной улицы, Вудхаус опубликовал фотографию с указателем на стене дома. «Где же ты, клавиатурный воин?», – написал Вудхаус. В ответ на это сообщение пользователь принес свои извинения. «Я ошибался и признаю это», – написал он. После этого боксер прекратил преследование пользователя.

Подготовлено по материалам «Lenta.ru»

НЕЗНАКОМЫЙ «ДРУГ»

При общении в онлайне всегда надо помнить, что под **ником**[3] может скрываться кто угодно, и приложенные фотографии ничего не значат.

Интернет – среда **условно анонимная**. Условно, потому, что в большинстве случаев вычислить ваш реальный IP-адрес, то есть сетевой адрес вашего компьютера, не составляет труда, а оттуда и до адреса офиса вашего интернет-провайдера совсем недалеко. Но все эти хитрые штуки доступны в основном полицейским, а вот простой пользователь своего собеседника знает только под ником и видит только на фотографиях.

А что если фотография новой «подружки», что очень хочет к Вам в гости «на чашку чая» «одолжена» у Анжелины Джоли, а на самом деле за ней скрывается отъявленный уголовник? Может «онлайн-жених», на фото, как две капли похожий на Бреда Пита и мечтающий петь серенады у Вас под окном, является серийным маньяком-убийцей? Очень даже может быть!

И, кстати, если «интернет-принц» живет «в тридевятом государстве», но ради Вас готов проскакать все эти тысячи миль, но исключительно за Ваш счет (ибо беден или имеет многочисленных родственников слабых здоровьем), это тоже повод задуматься. Но об этом чуть позже…

[3] Ник или никнейм/никнэйм (от английского «nickname» – «кличка» или «прозвище») – сетевое имя или псевдоним интернет-пользователя.

ЗНАЧИТ, ЗАПОМИНАЕМ ПРАВИЛА:

- Никогда не приглашайте новых «друзей» из Сети к себе домой!
  А если все же очень хочется познакомиться, что называется, «вживую» – встречайтесь в многолюдном месте, а после встречи не позволяйте себя провожать.
- Не забываем про правила из раздела «Социальные сети и Форумы».


@
SEND

ЭЛЕКТРОННАЯ ПОЧТА

«Я Вам пишу, чего же боле»

(С) А.С.Пушкин

Сегодня уже мало кто пишет бумажные письма родственникам и друзьям. Сейчас есть электронная почта. И хотя иногда электронная почта повторяет проблемы с пропажей писем и задержкой доставки своей старшей сестры – бумажной почты, в целом она быстрее и надежнее. А еще удобнее – никуда не надо идти, мучительно вспоминать индекс, клеить марки и облизывать конверт… Все делается не отходя от компьютера. Отправить маме фотографии из отпуска? Пожалуйста! Написать бухгалтеру о том, что он забыл оплатить счет за телефон, и теперь весь офис сидит без связи? Пожалуйста! И даже отправить письмо американскому Президенту – ничего не стоит, надо только знать электронный адрес[4] корреспондента.

Сервисов электронной почты сейчас развелось очень много, от предоставляемого вашим провайдером интернета, до бесплатных от «Яндекса» и «Мэйл.Ру». Надо только нажать кнопку «создать почтовый ящик», придумать логин и пароль, и опа! Пишите письма!

P.S. О паролях мы обязательно поговорим, но отдельно.

[4] Электронный адрес – выглядит как: имя пользователя (он же логин), которое пользователь придумывает сам, символ @ (собака), имя сервера, на котором находится почтовый ящик, точка и буквенное обозначение домена. Например, my@company.ru.

НЕПРИЯТНОСТИ

«СПАМ»

Спам – рассылка электронных писем (чаще рекламы) людям, не выражавшим желания их получать.

В общем-то, спам вполне безобидная штука, не приносящая особых неприятностей, кроме раздражения от замусоривания почтового ящика. Тем не менее, **спам может быть опасен**, важно, что у него внутри.

ПОЭТОМУ:

- Не поленитесь поставить галочку «защита от спама» в настройках вашего почтового ящика. Или хотя бы отмечайте такие письма как спам – это поможет вашей компьютерной почтовой программе распознавать спам еще на входе и не допускать его попадания в Ваш почтовый ящик.
- Никогда не отвечайте на спам и не переходите по указанным в нем ссылкам – это только даст понять спамерам, что на другом конце живой человек, и спровоцирует новый вал спама.

Внутренности электронных писем могут содержать:

«Трояны» и опасности «бот-нет»-сетей

Электронная почта отличный способ превратить Ваш компьютер в «бот» путем отправки Вам «трояна».

«Бот» (сокращение от «робот») – компьютер, зараженный специальной программой, позволяющей злоумышленнику управлять таким компьютером по своему усмотрению без согласия владельца компьютера. Из бот-компьютеров создаются бот-сети (бот-неты), занимающиеся, например, рассылкой спама или атакой на ресурсы банков, и все это при полном неведении хозяев таких компьютеров.

«Троян» («троянская программа») – вредоносная программа (компьютерный вирус), проникающая на компьютер пользователя под видом безобидного приложения с целью получить доступ к информации, размещенной на компьютере, или возможность удаленно управлять зараженной машиной.

ТАКИМ ОБРАЗОМ, СЛЕДУЮЩЕЕ ПРАВИЛО БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ ГЛАСИТ:

- Не открывай подозрительные и «нежданные» письма с неизвестных электронных почтовых ящиков, и, что особенно важно, не открывайте вложенные в них файлы.

- Письма с неизвестных Вам электронных почтовых ящиков, с ящиков со странными названиями и заголовками в теме сообщения, такие, например, как «Мария Вездесущая. Ваше желание исполнилось», и присланные в них файлы надо безжалостно удалять, не поддаваясь соблазну посмотреть, что там внутри.
- Обязательно установите на компьютер антивирусную программу.

«Нигерийские письма» или письма счастья»

Если Вам пришло письмо с текстом «Здравствуйте! Я Эрик Delanyo, практикующий юрист. Мой клиент г-н SRMoroshkin, который обнажает то же имя с вами и с вашей страной, но работал с зоны, Франш-Того (SAZOF) в качестве независимого древесины и фосфатов экспортер был убит со всей семьей в результате несчастного случая, не жалея ни своих жизни, несколько лет назад. До его внезапной смерти, я помогал ему в сдаче средств на сумму $9,5 млн., с частным банком на хранение. Эти средства остались невостребованными после его смерти, и такие невостребованные средства присваиваются и вернул в казну как вопрос политики. Учитывая отсутствие успеха в своей попытке определить местонахождение любого из его родственников в течение года теперь, я настоящим просить вашего согласия, чтобы я вам представить, как ближайших родственников моего покойного клиента…», поздравляем, Вы стали счастливым обладателем «нигерийского письма».

Канадский водитель грузовика Джон Ремпел из Лимингтона попался на удочку «бездетного английского однофамильца, жаждущего осчастливить кого-нибудь из Ремпелов наследством в 12,8 миллионов долларов».
Для начала от Джона потребовалось 2,5 тысячи долларов, чтобы осуществить перевод, потом еще 5 тысяч на оформление дополнительных документов, потом еще 5 тысяч на открытие счета в лондонском банке, потом выяснилось, что нужно оплатить налог размером в 250 тысяч, который усилиями доброго адвоката скостили до 25 тысяч… Потом были еще расходы на авиабилеты, расходы за услуги транспортной компании и т.д,. и т.д. «Сломался» Джон на взятке в 12500 долларов сотрудникам Нью-Йоркского аэропорта – только после этого он решил обратиться в полицию.
Всего на эти манипуляции у канадца ушло около 150 тысяч долларов.

Подготовлено по материалам РИА «Новости

«Нигерийские письма» или «письма счастья» – вид мошенничества, получивший распространения с появлением массовых рассылок писем по электронной почте.

Мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты от сумм. Если получатель письма, откликнулся и согласился участвовать, оказывается, что для получения «солидного куша» необходимо сделать самую малость – перевести немножко своих собственных денег на оформление сделки/уплату налогов/взятки чиновникам (нужное подчеркнуть)

и т.п. Естественно в результате жертва так и не получает никаких миллионов. Сравнительно недавно появились и российские аналоги «нигерийских писем», в которых переписка ведется от лица несуществующего «российского бизнесмена», якобы нуждающегося в помощи адресата в переводе своего огромного состояния из России в другую страну (разумеется, за щедрое вознаграждение).

Кроме варианта с «богатым дядей» существует вариант с лотереей – жертве сообщается о крупном выигрыше в лотерею. Получатель письма должен заплатить (например, налог), чтобы получить свой выигрыш. (С похожей схемой работают «лохотронщики» на российских площадях и вокзалах, «впаривая» копеечные утюг/духи/косметику как приз, за который надо заплатить 1000 рублей налога).

Также существует **онлайн-вариант брачной аферы**, в котором мошенники ведут любовную переписку с целью «создания семьи». Суть мошенничества заключается в выманивании относительно небольших сумм «на билет и визу» для встречи с «любимым» или просто на «покупку веб-камеры».

Каков бы ни был вариант обмана при помощи таких «писем счастья»

СОВЕТ МОЖЕТ БЫТЬ ТОЛЬКО ОДИН: НИКАКИХ ДЕНЕГ!

Какими бы заманчивыми не казались предложения, помните: если у Вас попросили денег – Вас наверняка «разводят» (ну то есть пытаются обмануть на деньги). Не пересылайте, не занимайте и не давайте денег таким знакомым без основательной проверки полученной информации и нотариально заверенной расписки.

«ФИШИНГОВЫЕ ПИСЬМА»

Фишинговые письма – еще один способ мошенничества при помощи электронной почты – заключается в **«выуживании»** (по английски fishing – рыбалка) у получателя письма **информации**, которую потом можно будет «монетизировать», например, адресов электронной почты других пользователей (их можно продать спамерам), паролей от других сервисов (социальных сетей, корпоративной электронной почты и т.д.).

На сегодняшний день преобладают фишинговые письма, направленные на **получение** от пользователя **номеров и паролей** его кредитных карточек или систем онлайновых платежей. Такие письма обычно маскируются под официальные сообщения от администрации банка, в которых сообщается, что получатель должен подтвердить сведения о себе (или срочно сменить пароль), иначе его счет будет заблокирован, и при-

водится адрес подставного сайта, внешне очень похожего на официальный сайт банка. Среди данных, которые необходимо ввести, есть и те, которые нужны мошенникам.

Чаще всего отличить «подставной» сайт от официального сайта банка «на глаз» практически нереально. Также простому пользователю очень сложно заметить разницу в доменных именах (символах, которые вводятся в адресную строку браузера для попадания на нужную интернет-страничку) этих сайтов.

О самих доменных именах мы поговорим отдельно.

ПОЭТОМУ ЗАПОМНИТЕ: ЛУЧШЕ «ПЕРЕБДЕТЬ», ЧЕМ «НЕДОБДЕТЬ»!

- Помните, банки или платежные системы НИКОГДА не запрашивают конфиденциальную информацию по электронной почте.
- Не переходите по ссылке, указанной в письме! Лучше наберите адрес сайта в браузере сами или найдите через поисковую систему (например, «Яндекс» точно знает официальные адреса сайтов крупных банков и умеет предупреждать о подозрительных сайтах).
- Внимательно читайте текст письма.
- Электронные письма от известных компаний не должны содержать орфографических или грамматических ошибок.
- Типичное фишинговое письмо начинается с обезличенного приветствия «Уважаемый пользователь» или обращения по адресу электронной почты. Ваш банк или платежная система обычно знает Ваше ФИО и в настоящем письме приветствует Вас, обращаясь по имени и фамилии (или имени и отчеству).
- Чаще всего мошеннические электронные письма содержат призывы к безотлагательным действиям (используя такие слова как «немедленно», «безотлагательно», «последнее предупреждение»), пытаясь заставить Вас действовать быстро и необдуманно.
- Не стесняйтесь позвонить в банк по номеру телефона, указанному на Вашей карте (именно на карте, а не указанному в письме или сайте, открывшемся по ссылке из письма, – там вполне может оказаться человек из команды мошенников) и все уточнить.
- Не пренебрегайте лицензионными антивирусами – многие из них блокируют фишинговые ссылки.
- Обращайте внимание на любые отклонения от обычного поведения Вашего банка (например, запрос новых сведений, которые раньше не надо было вводить). Если что-то идет не так как обычно, лучше отказаться от операции и перепроверить информацию у банка.
- Не пренебрегайте возможностью услуги «смс-оповещение» от банка – если деньги начнут внезапно утекать с Вашего счета, будет шанс успеть заблокировать карту.

ВЗЛОМ ПОЧТЫ

Здесь важно знать, что если кто-то очень хочет взломать Вашу почту (впрочем как и входную дверь Вашей квартиры) он это сделает. Это только **вопрос времени и затрат** ресурса человеческого или компьютерного (современные хакеры давно автоматизировали процесс взлома – это и быстрее и следов меньше).

КАК ОНИ ЭТО ДЕЛАЮТ?

- **Подбор пароля**
  Это самый простой (и самый используемый) способ вскрытия электронного почтового ящика. Для этого даже не надо быть программистом – в сети гуляет множество программ, которые подставляют в качестве пароля определенные слова (или сочетания символов) используя при этом готовые словари.

- **Подсматривание пароля**
  Подбор пароля – удел хакеров. А вот подсмотреть пароль, записанный на листочке, может случайно зашедший в гости сосед/коллега. Хорошо, если его любопытство ограничится просмотром Ваших фоток… Ну дальнейшее развитие событий можете додумать сами.

И ТУТ САМОЕ ВРЕМЯ ОЗВУЧИТЬ ОЧЕРЕДНЫЕ ПРАВИЛА:

«ПОДАЛЬШЕ ПОЛОЖИШЬ, ПОБЛИЖЕ ВОЗЬМЕШЬ»

(народная мудрость)

- Не храните в электронном почтовом ящике (особенно на бесплатном почтовом сервисе) ценную информацию, секретные документы и интимные фотографии. После пересылки или скачивания обязательно удаляйте такие письма. При необходимости переслать ценную для Вас информацию, воспользуйтесь программой шифрования, а код от шифра сообщите собеседнику другим способом, например, по телефону.
- Не используйте для паролей простые общеупотребимые слова.
- Никто не любит сложных паролей, так как их легко забыть, но если Вы не хотите, чтобы Вашу почту взломали хакеры, то правило - «чем сложнее пароль, тем выше безопасность» - именно для Вас.
- Если у Вас несколько почтовых ящиков, не используйте на всех один и тот же пароль. Пусть он будет отличаться на 1-2 символа, но это может спасти Вас от утечки всей информации.
- Не ленитесь периодически менять пароли, особенно в случае появления подозрения о том, что текущий вариант пароля скомпрометирован.
- НИ В КОЕМ СЛУЧАЕ не записывайте пароли в блокнотике, который лежит «под рукой» возле монитора компьютера.

МЕССЕНДЖЕРЫ

(программы для мгновенного обмена сообщениями – «Skype», «ICQ» и др.)

Переписка при помощи **мессенджеров** содержит такие же **опасности**, как и переписка по электронной почте: рассылка спама, фишинг, заражение компьютера вирусами.

Иногда мошенники могут обратиться к Вам от лица Вашего друга, **взломав** его **учетную запись** и попросить переслать деньги на определенный счет или телефонный номер… Конечно бывают ситуации, когда другу действительно требуется срочно пополнить баланс, например, мобильного телефона, поэтому такие просьбы лучше перепроверить личным телефонным звонком или контрольным вопросом, ответ на который не может знать посторонний человек.

А в целом правила поведения при общении через мессенджеры полностью повторяют правила работы **с электронной почтой**.

«ФЕЙКИ[5]»

«Ах, обмануть меня не трудно!..

Я сам обманываться рад!»

(С) А. С. Пушкин

Людей во все времена обманывали – продавали эликсир вечной жизни, обещали кару богов за непочтение к властителю, сулили золотые горы в походе за тридевять земель, рассказывали небылицы про трехглавых драконов… Цели при этом преследовались абсолютно разные – от «просто так, ради красного словца», до зарабатывания на этом миллионных состояний (помните историю с МММ?). Появление интернета значительно упростило работу профессиональных обманщиков. Возможность скрыть свое имя за ***«ником»****, а истинное лицо - за чужой фотографией позволяет особо не бояться возмездия за свой обман, а умение пользоваться «анонимайзерами[6]» вообще делает интернет-обманщика практически неуловимым.*

[5] Фейк – (от английского «fake») подделка, фальсификация, подлог, обман.

[6] Анонимайзер – техническое или программное средство для скрытия информации о компьютере или пользователе в Сети.

В июне 2014 года на электронную почту российских и иностранных информационных агентств со ссылкой на пресс-службу Правительства Российской Федерации пришло сообщение об отставке главы РЖД Владимира Якунина со своего поста. За короткое время эта «горячая» новость облетела все крупные и множество небольших информагентств и новостных сайтов, ведь практика сообщать о различных решениях как Президента России, так и Правительства РФ через рассылку официальных документов по E-mail довольно распространена. При этом в телефонных беседах никто из официальных лиц факт отставки подтвердить или опровергнуть не мог. Новость вызвала удивление даже у пресс-секретаря самого «уволенного» топ-менеджера. Примерно через час после публикации новости появляется новая информация, сообщающая о том, что пресс-служба Белого дома факт рассылки пресс-релиза об отставке не подтверждает. Российские СМИ замирают в тревожном ожидании официального заявления. В это время специалисты одного из СМИ обнаруживают, что пресс-релиз пришел с электронной почты, IP-адрес которой не совпадает с IP-адресом почтового сервиса пресс-службы Правительства России. И, наконец, еще через некоторое время на информационных лентах появляется «молния» от пресс-секретаря премьер-министра, которая сообщает, что разосланная информация об отставке является фальшивкой. Дальнейшее расследование показало, что сообщение об отставке пришло с сайта, доменное имя которого было очень схоже с именем сайта Правительства РФ (aprf.gov.ru – домен Белого дома, aprf-gov.ru – домен, с которого было выслано сообщение). Сам сайт располагался на сервере иркутского интернет-провайдера. Гражданин, арендовавший сервер, сделал это онлайн и указал фальшивые личные данные.

Подготовлено по материалам газеты «Известия»

НЕПРИЯТНОСТИ:

«ФЕЙКОВЫЕ» НОВОСТИ

В последнее время в Сети появилось много так называемых «фейк»новостных сайтов – сайтов, распространяющих качественно сделанные **«ложные» новости**.

Такого рода **псевдо-новости** в интернет могут «вбрасывать» специальные сайты, основным предназначением которых является создание и распространение «фейков». Лженовости могут появляться в результате намеренной попытки распространить «фейк» (главным фактором распространения такого новостного контента[7] является банальная погоня за сенсацией, в результате которой онлайн-издания получают интернет-трафик, клики, внимание пользователей и, как следствие, рост цен на размещаемую рекламу), либо после взлома медиа и вбрасывания дезинформации.

[7] Контент – обобщенное название всего того, что можно скачать (посмотреть, почитать, послушать и т.д.) в интернете (программы, тексты, фильмы и др.).

ТУТ ЛУЧШЕЕ ПРАВИЛО: ДОВЕРЯЙ, НО ПРОВЕРЯЙ!

Без потребителя, без аудитории, заинтересованной в такого рода лже-сенсациях, «фейковые» новости не имели бы смысла. Ведь это мы делаем «перепосты» «сенсационных» новостей, «расшариваем» их и активно обсуждаем в соцсетях…
Так вот, прежде чем все это делать, было бы неплохо проверить информацию… Хотя истины ради, следует отметить, что зачастую это очень трудно сделать. Ну тогда хотя бы подождите немного, прежде чем самозабвенно бросаться «под орудия информационной войны», возможно в ближайшее время появится официальное опровержение…

«ФЕЙКОВЫЕ» ОБЪЯВЛЕНИЯ С ПРОСЬБОЙ О ПОМОЩИ

Помните в «Одноклассниках» Вас просили «перепостить» (разместить у себя на страничке в социальной сети) объявление о том, что милый котенок или щенок срочно ищет своего хозяина, а то иначе его придется утопить или усыпить, так как денег на его содержание нет, а к объявлению прикладывалась умильная фотка несчастной «животинки» и номер телефона его нынешнего владельца? Так вот, вполне возможно это «развод»! «Развод» – в смысле **попытка «развести»** Вас, ну или говоря языком Уголовного кодекса Российской Федерации – попытка мошенническим путём завладеть Вашими денежными сбережениями. Каким образом?

Например, звонок на указанный номер телефона может оказаться платным… Или на том конце провода Вам поведают слёзную историю, сводящуюся к тому, что, чтобы забрать питомца, Вы должны сначала перечислить/выслать небольшую сумму…

А еще возможен современный **интернет-вариант липового инвалида**, просящего «деньги на лечение», под объявлением которого стоит логотип известного благотворительного фонда, а вот реквизиты счета не имеют к нему никакого отношения…

ПРАВИЛО: ПРЕЖДЕ ЧЕМ СДЕЛАТЬ ДОБРОЕ ДЕЛО, ПОДУМАЙ!

Мы ни в коем случае не говорим, что все такие объявления являются делом рук мошенников, и что не надо помогать «братьям нашим меньшим» и не призываем Вас не тратить деньги на благотворительность. Мы призываем не верить огульно всем подряд, не делать «перепост» любых объявлений с просьбой о помощи.
Мы призываем Вас думать! Думать и проверять информацию! Это значит переводить деньги проверенным и хорошо известным благотворительным фондам, брать реквизиты благотворительных организаций на их официальных сайтах, размещать на своей страничке в соц. сети объявления о требующейся помощи «из первых рук» от людей, которым Вы доверяете.

Ну или если Вам ну очень уж хочется помочь именно этой никому неизвестной организации или милой собачке – «пробейте» через интернет-поисковик информацию по названию организации или указанному в объявлении номеру телефона – возможно кто-то уже отписался, как попался на удочку мошенников… а может, стал владельцем замечательного симпатичного домашнего питомца.

«ФЕЙКОВАЯ» РАБОТА

Интернет пестрит объявлениями о **вакансиях на «удаленку»** – работу из дома через сеть интернет. Работать, «не вставая с дивана», и еще получать за это приличные деньги – это ли не мечта? И хотя мечты таки сбываются, иногда они все же выходят соискателю «боком»…

При поиске удалённой работы, например, наборщиком текста, можно стать **жертвой** так называемых **«анкетников»**. После того, как Вы изъявили желание занять указанную в объявлении вакансию, Вам приходит приглашение от работодателя, в котором он предлагает Вам заполнить регистрационную форму (анкету), после заполнения и отправки которой Вам предлагается перевести 30-50 рублей (в зависимости от запросов мошенника). Это объясняется либо необходимостью оплачивать труд людей, обрабатывающих анкеты, либо просто тем, что Вы должны таким образом «подтвердить свои намерения работать» и что Вы не бросите все, в то время как «работодатель» на Вас очень надеялся. Как правило, деньги просятся небольшие, а перспектива получить хорошую «непыльную» работу сильна, поэтому многие переводят деньги. Естественно, как только Вы переведете деньги – про Вас навсегда забудут.

Похожий вид мошенничества с «удалёнкой» – предложение работы региональным представителем. Некая фирма предлагает Вам стать её эксклюзивным **региональным представителем**. После успешного прохождения собеседования Вам объявляют, что Вы приняты и что все необходимые документы (договор о сотрудничестве и т.д.) придут к Вам заказной почтой (что обычно и происходит). После получения извещения о заказном письме, на почте вдруг выясняется, что направлено оно **наложенным платежом**… Желание работать «на теплом местечке» и небольшой размер требуемой суммы делают свое дело, и Вы становитесь «счастливым» обладателем бланка трудового договора… На этом сотрудничество скорее всего и закончится – никто не будет присылать Вам задания и, соответственно, оплачивать Вашу работу.

Тестовые задания – это самый безобидный способ обмана (здесь Вы хотя бы ничего не потеряете, кроме своего времени). В этом варианте никто не просит Вас что-то оплатить вперед. Просто на собеседовании соискателю предлагают выполнить тестовую работу (напечатать текст, перевести письмо, «набросать» проект и т.д.), которая так и останется неоплаченной, так как соискатель «к нашему большому сожалению» не прошел по конкурсу.

ПРАВИЛА:

- Никаких денег с Вашей стороны! Помните, это Вы выполняете работу, и, значит, это Вам должны заплатить!
- Поищите в поисковике компанию, предлагающую Вам работу – такие схемы обмана рассчитаны на большое количество доверчивых и беспечных пользователей, и есть шанс не попасть в их число благодаря отзывам интернет-пользователей.
- Пользуйтесь проверенными сайтами вакансий:
  многие сайты ответственных рекрутинговых компаний имеют свои базы проверенных работодателей и не позволяют размещать на своих страницах вакансии от «непонятных личностей»
  кроме того, в Сети есть хорошо зарекомендовавшие себя сервисы в помощь свободолюбивым труженикам – фрилансерам (например, такие, как «freelance.ru», «fl.ru», «copylancer.ru»).
  наличие в качестве реквизитов организации только электронной почты должно сразу насторожить Вас и навести на мысль о возможном мошенничестве.

ИНТЕРНЕТ-МАГАЗИНЫ И СЕРВИСЫ ГРУППОВЫХ ПОКУПОК

– Утром деньги – днём стулья,
днём деньги – вечером стулья...
– А можно наоборот?
– Можно, но деньги вперёд!

© из к/ф «12 стульев»

С прогрессом ритм жизни жителя мегаполиса ускоряется. Нам уже некогда стоять у плиты и ходить по магазинам, и мы заказываем еду с доставкой на дом и покупаем товары в интернет-магазинах (в том числе и зарубежных).
Покупка в интернет-магазине иногда походит на покупку кота в мешке – никогда не знаешь совпадет ли то, что ты выбрал с тем, что тебе привезут. Чего стоит хотя бы фраза: «Производитель оставляет за собой право изменять конструкцию, технические характеристики, внешний вид, комплектацию товара, не ухудшающие его потребительских качеств, без предварительного уведомления потребителя!» Но это, конечно, не самое страшное. Хуже если Вы останетесь вообще без товара, заплатив при этом какие-то деньги, или вообще без денег… Всех денег!
Мы не будем здесь рассматривать случаи воровства денег при помощи скиммеров[8] и фальшивых банкоматов – это не задача нашего материала. Здесь мы говорим только о неприятностях поджидающих Вас в Сети.

[8] Скиммер – специальное считывающее устройство, с помощью которого мошенники копируют информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания срока ее действия, CVV- и CVC-код).

НЕПРИЯТНОСТИ

НЕПОСТАВКА ПРЕДОПЛАЧЕННОГО ТОВАРА

Многие интернет-магазины принимают оплату товара онлайн – то есть Вы сначала оплачиваете выбранный товар с **электронного кошелька** (например, через «Яндекс. Деньги») или пластиковой карты, а уже после этого продавец высылает Вам товар.

В этом случае самый простой способ обмана покупателя – получив деньги, «скрыться в неизвестном направлении», и интернет позволяет сделать это как нельзя лучше – достаточно просто перестать отвечать на звонки и электронные письма.

Другой способ обмана через интернет-магазин – привезти **«серый»** или заведомо **неисправный товар** с последующим отказом его ремонтировать или принимать обратно в случае поломки. Некоторое время назад это было достаточно массовое явление для российской интернет-торговли. Онлайн-магазины почему-то считали (а некоторые по-прежнему придерживаются этого же подхода к своему бизнесу), что Закон «О защите прав потребителей» на них не распространяется, а значит выполнять его не обязательно. Сейчас ситуация вроде бы более-менее нормализовалась, но «в семье ж не без урода»…

ПРАВИЛА ПРИ ОНЛАЙН-ПОКУПКАХ:

Все же лучше «сначала стулья»

- по возможности не производите предоплату покупок
- многие (а в Москве большинство) российские интернет-магазины позволяют оплатить товар курьеру после его доставки и проверки.

Хороший продавец = надежный продавец

- покупайте на проверенных сайтах (по рекомендациям знакомых и друзей). При покупке из-за рубежа обращайтесь к известным крупным интернет-магазинам («Amazon», «Ebay» и др.) – они дорожат своей репутацией и имеют свою систему безопасных покупок, позволяющую вернуть деньги;
- если выбираете товар в российском интернет-магазине через «Яндекс. Маркет» почитайте отзывы о продавце. При участии в групповой покупке проверяйте рейтинги и отзывы о её организаторе;
- требуйте у продавца товарный чек – стопроцентной гарантии того, что в случае чего продавец заменит Вам негодный товар, нет, но без него Ваши шансы на замену или возврат денег резко сокращаются.

СБОР ПЕРСОНАЛЬНЫХ ДАННЫХ

Некоторые онлайн-магазины требуют указать на сайте не только номер телефона «для связи», но и еще множество другой информации, абсолютно не пригодной для целей покупки конкретного товара в конкретном магазине (ну зачем например интернет-магазину Ваше отчество?!). Мы не знаем точно, но похоже это какой-то попутный бизнес электронных продавцов – **собрать побольше** данных о своих покупателях, а затем **продать** их куда-то на сторону неизвестному спамеру или неугомонному call-центру.

И ТУТ СЛЕДУЕМ ПРАВИЛАМ: ЛИШНИХ ДАННЫХ НЕ БЫВАЕТ? НЕ В ВАШЕМ СЛУЧАЕ!

- Если заказываете товар с доставкой курьером, ограничьтесь указанием имени и номера мобильного телефона для связи (ну если уж продавец настаивает на необходимости указать все Ваши данные, опишите себя как Иванова Ивана Ивановича);
- если заказать товар без указания дополнительной информации о себе невозможно, лучше выбрать другого продавца (попутно не лишним будет написать жалобу в Роскомнадзор о незаконном сборе персональных данных, благо сейчас это можно сделать, не выходя из дома).

СБОР ДАННЫХ ПЛАТЕЖНЫХ КАРТ ПОКУПАТЕЛЕЙ С ЦЕЛЬЮ ДАЛЬНЕЙШЕЙ КРАЖИ РАЗМЕЩЕННЫХ НА НЕЙ СРЕДСТВ

Технологии **интернет-торговли** для этого подходят как нельзя лучше. Часто до получения реального товара дело так и не доходит. В этом плане подозрительными являются заманчивые предложения о продаже ходовых товаров или услуг с несоизмеримыми с реальной ценой товара скидками, о бесплатной рассылке товара с предоплатой по карте клиента только почтовых затрат.

Другим методом является создание **подложной страницы сайта** известного интернет-магазина или фишингового сайта.

ПОЭТОМУ НЕ ЗАБЫВАЕМ ПРАВИЛА:

НЕ КЛАДИТЕ ВСЕ ~~ЯЙЦА~~ ДЕНЬГИ В ОДНУ КОРЗИНУ!

- Заведите себе отдельную пластиковую карту для оплаты покупок через интернет, на которую переводите достаточную сумму непосредственно перед покупкой – так Вы сохраните остальные Ваши сбережения от пронырливых интернет-воришек.
- Стоит хорошенько запомнить, что сайты «приличных» электронных платежных систем всегда защищены сертификатами SSL. То есть если адрес сайта, через который Вы хотите провести оплату, начинается с «http://» (обычный интернет-протокол) вместо «https://» (защищенный интернет-протокол), то это гарантировано подделка.
  + все то, что написано в разделе «Фишинговые письма».

ИНТЕРНЕТ (ОНЛАЙН)-БАНКИНГ ИЛИ МОБИЛЬНЫЙ БАНК

Лень – двигатель прогресса!

Да, именно так. Нам лень для перевода денег идти в банк, стоять в очереди к операционисту… и вот мы уже оправляем деньги другу с банковской карты, не отрываясь от чашки кофе и просмотра любимого сериала, или оплачиваем родителям мобильную связь, направляясь на работу в метро… В последние годы для удобства клиентов банки автоматически подключают при оформлении карты (или через некоторое время после оформления) такую услугу, как пополнение баланса мобильного телефона со счета карты. Причем для совершения такой операции необходим только сам телефон, к номеру которого привязана карта. Да, несомненно, новые сервисы по доступу к банковскому счету со смартфона очень удобны, но они таят в себе немалую опасность остаться без средств.

НЕПРИЯТНОСТИ:

УТРАТА ТЕЛЕФОНА

Даже если у Вас не стоит мобильное приложение онлайн-банкинга, поставить его не составит особого труда. А **смс-оповещения** от Вашего банка будут приходить именно на этот телефон, находящийся в руках врага.

ЗАРАЖЕНИЕ СМАРТФОНА ВИРУСОМ, ВОРУЮЩИМ ДЕНЬГИ

Апрель 2015 г.
Управлением «К» МВД России при содействии экспертной организации и службы безопасности Сбербанка задержаны российские участники одной из киберпреступных групп. Злоумышленники организовывали вирусные атаки на мобильные устройства клиентов российских банков.
Троянская программа, которую они использовали, после установки на мобильное устройство запрашивала баланс привязанной к номеру банковской карты, скрывала поступающие SMS-уведомления и осуществляла переводы денежных средств с банковского счета на счета, подконтрольные злоумышленникам.
На основании полученных данных удалось установить личности четырех жителей Челябинской области, подозреваемых в совершении преступления. У задержанных было изъято несколько ноутбуков, полтора десятка сотовых телефонов и большое количество SIM-карт.

Подготовлено по материалам журнала «Computerworld»

ПРАВИЛА: ВОТ ТУТ МЫ СКАЖЕМ, КАЗАЛОСЬ БЫ, СТРАННУЮ ВЕЩЬ, НО…

- если у вас к счету мобильного телефона привязана банковская карта, то в случае утраты мобильного телефона обязательно и срочно блокируйте не только сим-карту, но и банковскую карту (в крайнем случае позже ее можно будет разблокировать).
- А прямо сейчас поставьте на Ваш смартфон антивирусное приложение.

ТОРРЕНТЫ[9] И ФАЙЛООБМЕННИКИ[10]

«На халяву и уксус сладкий»

(С) русская народная поговорка.

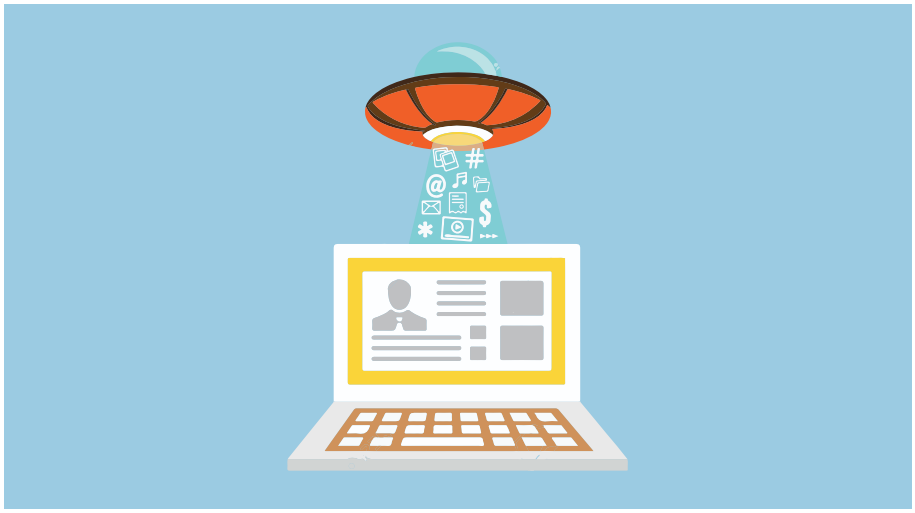
Принимая решение качать фильм или книгу через торрент-трекер надо помнить, что в Российской Федерации (а равно и в других цивилизованных странах мира) авторское право защищено законом! Это значит, что за незаконное размещение (а кое-где и за скачивание) фильма, книги, музыки и другой подобной информации с нарушением чужих авторских прав можно «огрести» реальный штраф или даже срок заключения.
Если сомневаетесь в «чистоте» авторских прав скачиваемого файла лучше поискать другие, легальные способы получить нужную информацию. Например, воспользоваться сайтом «онлайн-кинотеатр», где недорого (а может и бесплатно, но при наличии рекламы) можно посмотреть приглянувшийся фильм.
Но мы сейчас не об этом…

Атрибутом защищаемого авторским правом контента (будь то текст, картинка или что-то еще) является знак копирайта латинская буква С в окружности – © или полукруглых скобках – (С), вместе с именем правообладателя и годом публикации.
Но существует еще контент, защищаемый «свободной лицензией» (free license) – это такой лицензионный договор, условия которого содержат разрешения пользователю от правообладателя на конкретный перечень способов использования его произведения (наиболее популярный формат свободной лицензии – лицензия «Creative Commons» – изображается в виде букв CC в кружочке или полукруглых скобках).
P.S. Немного о копирайте и свободных лицензиях читайте в дополнительных материалах.

---

[9] Торрент – система передачи файлов (файлового обмена между пользователями) с использованием специального программного обеспечения. Особенность этой системы в том, что файлы передаются частями с компьютеров пользователей уже скачавших файл, при этом скорость закачки напрямую зависит от количества таких компьютеров. После закачки всех частей файла торрент-программа (торрент-трекер) собирает его в одно целое.

[10] Файлообменник – это сервис, на котором пользователь может разместить свой файл (или несколько файлов) в интернете, а взамен получить ссылку (гиперссылку), по которой этот файл будет круглосуточно доступен всем, кому она будет известна.



НЕПРИЯТНОСТИ:

ВИРУСЫ, СПРЯТАННЫЕ ВНУТРИ АРХИВОВ С ФИЛЬМАМИ

Про вирусы и о том, какое это зло, Вы, наверное, уже и так знаете…

КРАЖА ДЕНЕГ С ТЕЛЕФОНА

При попытке найти в интернете **бесплатный контент** в виде фильма или программного обеспечения пользователи периодически натыкаются на сайты, предлагающие **ввести номер** мобильного телефона. Выглядит это примерно так: «Напишите номер своего мобильного, Вам придет смс с кодом (или ссылкой), подтвердите ее получение ответной смс-кой (или нажмите на ссылку) и будет Вам счастье в виде фильма». Объясняется это защитой от «ботов», но на самом деле вполне возможно, что Вас подпишут на платную рассылку или спишут Н-ную сумму со счета телефона, а нужного файла Вы так и не увидите.

ЧТОБЫ НЕ ПОПАСТЬСЯ «НА УДОЧКУ» СОБЛЮДАЙТЕ ПРАВИЛА: НЕ ВВОДИТЬ НОМЕР МОБИЛЬНОГО ТЕЛЕФОНА НА СОМНИТЕЛЬНЫХ САЙТАХ.

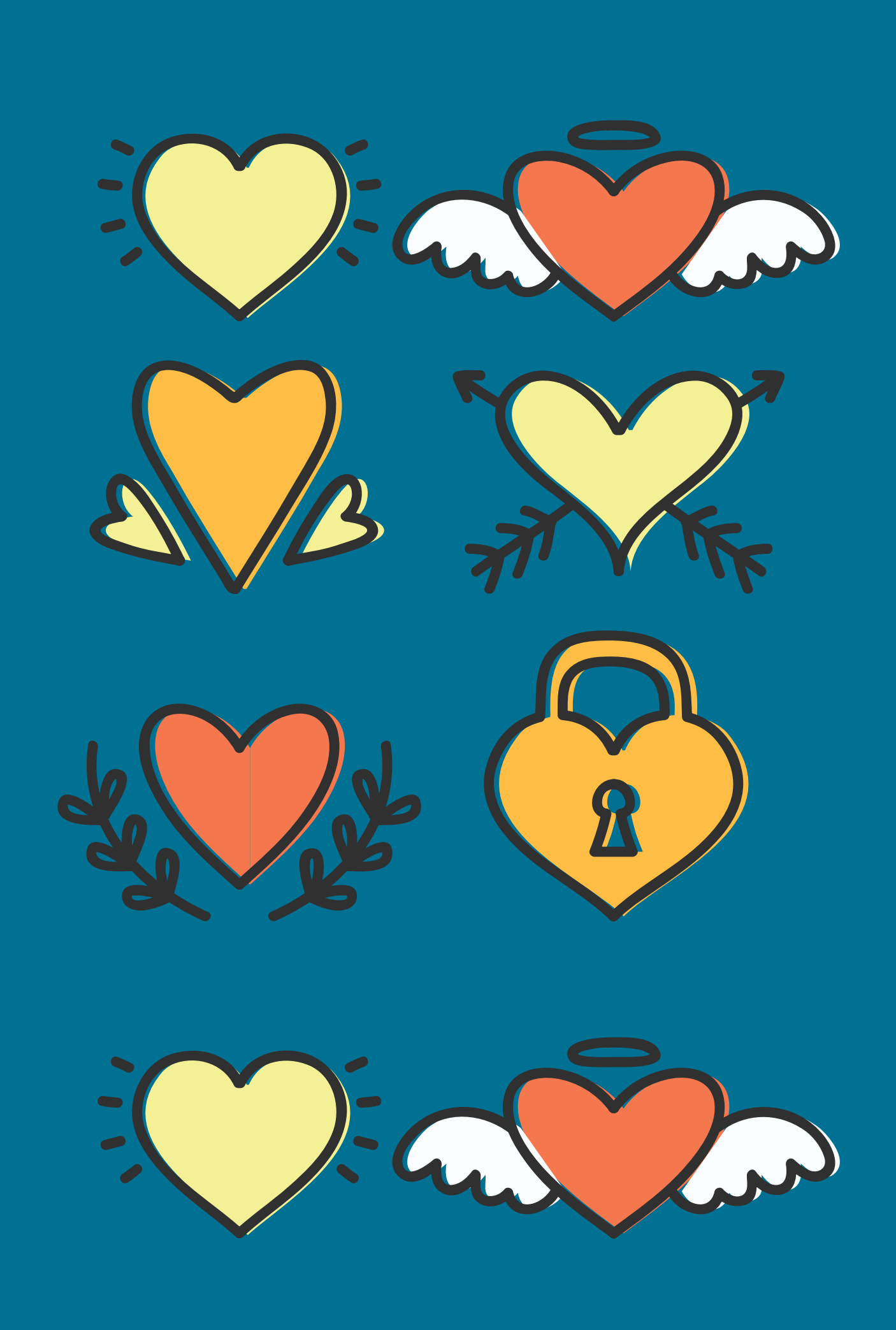
Часто тут же мошенники размещают сообщение якобы от лица другого пользователя, который утверждает, что прошел все требуемые процедуры и уже скачал файл, и ничего страшного не случится, если вы сделаете то же самое. Не верьте!

НЕ ОТПРАВЛЯЙТЕ ОТВЕТНЫХ СМС И НЕ АКТИВИРУЙТЕ ПРИШЕДШИЕ ССЫЛКИ.

Некоторые популярные сайты («Одноклассники», «ВКонтакте») для дополнительной защиты просят указать номер мобильного телефона, на который потом присылают код, который надо ввести НА САМОМ САЙТЕ, но ни в коем случае не отправить ответной смс-кой.

Кстати, для обеспечения безопасности Вашего мобильника от различных денежных подписок рекомендуем заблокировать такую возможность через Вашего мобильного оператора.

Ну и повторим еще раз – антивирус должен быть на Вашем компьютере!



САЙТЫ ДЛЯ ВЗРОСЛЫХ

Любителям «клубнички» посвящается...

Мы же с Вами взрослые люди? Поэтому говорить здесь о том, что смотреть порнографию это ой-ёй-ёй как нехорошо мы не будем. Поговорим лучше о том, как не пострадать при этом материально.

НЕПРИЯТНОСТИ:

ПЛАТНЫЙ КОНТЕНТ

Собственно это вряд ли можно отнести к неприятностям. Это не только достаточно распространенная во всем мире практика, но и способ оградить детей от получения нежелательной для них информации (не зря же на такой информации пишут «Только для взрослых» или ставят значок «18+»). Просто будьте готовы к тому, что за просмотр «горячего» видео Вас попросят заплатить.

И СНОВА ВИРУСЫ

Некоторое время назад **сайты с контентом для взрослых** были основным распространителем компьютерных вирусов, а первое, что говорили человеку с зараженным компьютером, так это: «А не надо ходить на порносайты!». Сейчас эта индустрия стала несколько более цивилизованной (и даже появился целый отдельный домен верхнего уровня .XXX), но вирусы по-прежнему не дремлют.

КОМПРОМЕТАЦИЯ ЛИЧНОСТИ, ШАНТАЖ И ВЫМОГАТЕЛЬСТВО

Если Вы являетесь публичной известной личностью – политик, актёр – (да даже если не являетесь!) освещение фактов просмотра «взрослого видео» или занятия «виртуальным сексом» может нанести **непоправимый урон** вашей репутации или семейной жизни. Кроме того, есть вероятность стать объектом шантажа и вымогательства со стороны, предоставляющей интимные услуги через интернет.

В 2012 году несколько россиян стали жертвами виртуальных шантажистов. Вымогатели требовали перевода определенных денежных сумм (от 2-х до 5-ти тысяч рублей) за нераспространение компрометирующего видео. Злоумышленники действовали по следующей схеме: через социальную сеть пострадавшим поступало предложение заняться виртуальным сексом с использованием веб-камеры. В случае согласия жертвы, злоумышленники вступали в диалог, выпытывая максимум информации (номера телефонов, реальные имя и фамилию и т.д.).

Через некоторое время после виртуального секса потерпевшему поступали предложение выкупить видео, которое злоумышленник записал во время сеанса. В случае неперечисления денег преступники угрожали распространить компрометирующее видео всем контактам потерпевшего.

Подготовлено по материалам информационного агентства

Другой известный вариант вымогательства – когда после предоставления виртуальной интимной услуги через Skype девушка внезапно признается, что ей еще нет 18 лет, после чего следуют угрозы обвинить в совращении малолетних.

ЧТО ЖЕ ТУТ МОЖНО ПОСОВЕТОВАТЬ?

Способы защиты сбережений при оплате «видео для взрослых» мало чем отличаются от банальной покупки через интернет (см. раздел, посвященный интернет-магазинам).

- Обязательно установить антивирус.
- Не передавать свои персональные данные
- в данном случае под «персональными данными» мы подразумеваем не только Ваши фамилию, имя и отчество, но и номер телефона, адрес странички в социальной сети и др. Кроме того, неплохо было бы ограничить круг обзора веб-камеры таким образом, чтобы туда не попало Ваше лицо.
- Если Вы все же стали объектом вымогательства, необходимо обратиться с заявлением в правоохранительные органы, так как деяния такого рода подпадают под признаки состава преступления, предусмотренного ст. 163 Уголовного кодекса Российской Федерации.

ДОПОЛНИТЕЛЬНЫЕ МАТЕРИАЛЫ:

ПАРОЛИ

Процесс придумывания (и главное, запоминания) сложных паролей можно упростить, если вспомнить, что наши клавиатуры имеют две раскладки – русскую и латинскую. Например, простой пароль «password» можно переиначить в «gfhjkm», то есть русское слово «пароль» набрать в латинской раскладке клавиатуры. А можно еще больше усложнить задачу по подбору пароля путем использования целых фраз, заменяя пробелы между словами какими-либо специальными символами (например, пароль «мама мыла раму» легко трасформируется в «vfvf$vskf$hfve$»). Добавляем смену регистров (большие и маленькие буквы), цифры и сильно осложняем дело противным хакерам.

ДОМЕННЫЕ ИМЕНА

Доменное имя – это то имя сайта, которое Вы видите (или набираете) в строке браузера (например «yandex.ru» или «президент.рф»).

Есть доменные имена (или попросту «домены») верхнего уровня (корневые домены), такие как «.ru», «.com» или кирилический домен верхнего уровня «.рф», и домены второго уровня («mail.ru», «спутник.дети»), и даже третьего уровня («neva.spb.ru», «fms.gov.ru»).

Чтобы разместить на домене свой сайт, его надо сначала зарегистрировать, для этого есть специальные компании – регистраторы. У каждого домена есть свой администратор – человек зарегистрировавший на себя доменное имя и определяющий политику использования домена.

Вообще регистрация доменных имен это целая отдельная индустрия. И если Вам интересно, то более подробную информацию о доменных именах можно прочесть на странице администратора российских доменов верхнего уровня «.RU» и «.РФ» – Координационного центра национальных доменов RU и РФ (http://cctld.ru).

ЗНАК КОПИРАЙТА © И СВОБОДНАЯ ЛИЦЕНЗИЯ

Знак копирайта © оповещает пользователя о том, что права правообладателя данного контента защищены законодательством об авторском праве. А это значит, что Вы не можете использовать контент по своему усмотрению без разрешения правообладателя. Так, например, большинство СМИ разрешают перепечатку своих авторских текстов при условии указания ссылки на первоисточник, а вот

профессиональные фотографы, заработок которых напрямую зависит от числа копий сделанных ими фотографий, запрещают любое бесплатное использование своих авторских произведений.

Таким образом, наличие знака © однозначно говорит о том, что на использование контента наложены какие-то ограничения. Вместе с тем, отсутствие знака копирайта не говорит о том, что данный контент можно свободно использовать.

Для обозначения возможности свободного использования авторских произведений были придуманы свободные лицензии, например свободная лицензия на программное обеспечение (так называемое СПО – свободное программное обеспечение) или свободная лицензия на произведения культуры «Creative Commons» (CC). Свободные лицензии также могут налагать некоторые ограничения на использование контента – например, запрет использования произведения в коммерческих целях.

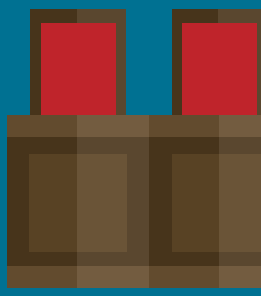
В любом случае помните, что бездумное использование чужого авторского произведения может привести к проблемам с законом.

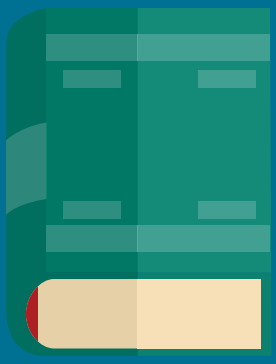
БЕЗОПАСНОСТЬ НАШИХ ДЕТЕЙ

На тему обеспечения безопасности подрастающего поколения в Сети интернет есть немало исследований, статей и книг.

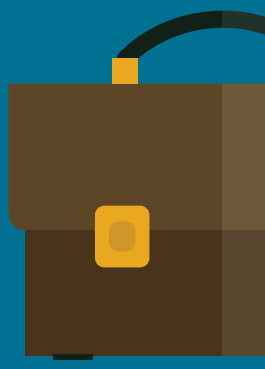
Не останавливаясь на этом подробно, скажем только, что если Вам не безразлична судьба Вашего ребенка (или внука), то установка на Вашем компьютере и использование фильтра родительского контроля – это обязательный элемент обеспечения безопасности ребенка, такой же важный, как объяснение правил перехода улицы.

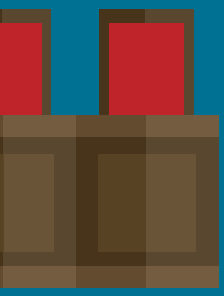






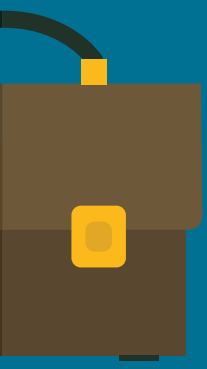


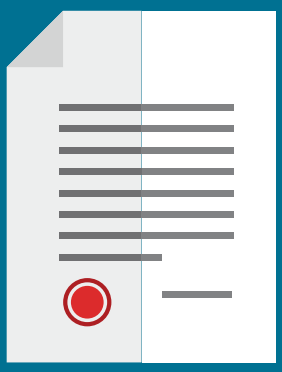




ИНТЕРНЕТ И РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО

«Dura Lex Sed Lex» –
«Закон суров, но это закон»





ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 Г. № 149-ФЗ «ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ»

ОСНОВНЫЕ МОМЕНТЫ:

СТАТЬЯ 15.1. ЕДИНЫЙ РЕЕСТР ДОМЕННЫХ ИМЕН, УКАЗАТЕЛЕЙ СТРАНИЦ САЙТОВ В СЕТИ "ИНТЕРНЕТ" И СЕТЕВЫХ АДРЕСОВ, ПОЗВОЛЯЮЩИХ ИДЕНТИФИЦИРОВАТЬ САЙТЫ В СЕТИ "ИНТЕРНЕТ", СОДЕРЖАЩИЕ ИНФОРМАЦИЮ, РАСПРОСТРАНЕНИЕ КОТОРОЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ ЗАПРЕЩЕНО:

Часть 5

Основаниями для включения в реестр сведений являются:

1. решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети "Интернет":
   а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;
   б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, местах приобретения таких средств, веществ и их прекурсоров, о способах и местах культивирования наркосодержащих растений;
   в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;
   г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;
   д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года N 244-ФЗ "О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации" и Федерального закона от 11 ноября 2003 года N 138-ФЗ "О лотереях" о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети "Интернет" и иных средств связи;
2. Вступившее в законную силу решение суда о признании информации, распространяемой посредством сети "Интернет", информацией, распространение которой в Российской Федерации запрещено.

СТАТЬЯ 15.2. ПОРЯДОК ОГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ, РАСПРОСТРАНЯЕМОЙ С НАРУШЕНИЕМ АВТОРСКИХ И (ИЛИ) СМЕЖНЫХ ПРАВ

Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети “Интернет”, объектов авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемых в таких сетях, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие объекты или информацию, на основании вступившего в силу судебного акта.

СТАТЬЯ 15.3

В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети “Интернет”, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, включая случай поступления уведомления о распространении такой информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители направляют требование в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

СТАТЬЯ 17, ЧАСТЬ 1

Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

Что размещение всей указанной информации карается по закону (где-то Уголовным Кодексом РФ, где-то Кодексом об административных правонарушениях, ну а где-то блокировкой сайта…).

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 27.07.2006 Г. № 152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

ОСНОВНЫЕ МОМЕНТЫ:

СТАТЬЯ 3, ПУНКТЫ 1 И 3

персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

СТАТЬЯ 6, ЧАСТЬ 1, ПУНКТ 1

обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.

СТАТЬЯ 7

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

Все Ваши персональные данные (фамилия, имя, отчество, адрес проживания и т.д.) могут собираться и распространяться только с Вашего разрешения. Если вдруг Вы обнаружите в сети интернет информацию о себе, содержащую Ваши персональные данные, разрешение на размещение которых Вы не давали, требуйте от владельца сайта её удаления. А в случае, если Вам отказывают в удалении – обращайтесь в Роскомнадзор (см. ссылку ниже), в полномочия которого входят такие вопросы.

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 29.12.2010 Г. № 436-ФЗ

«О ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ» И «ПРАВИЛА ОКАЗАНИЯ УСЛУГ СВЯЗИ ПО ПЕРЕДАЧЕ ДАННЫХ (УТВЕРЖДЕНЫ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 23.01.2006 Г. № 32)»

ОСНОВНЫЕ МОМЕНТЫ:

СТАТЬЯ 14, ЧАСТЬ1 ФЕДЕРАЛЬНОГО ЗАКОНА

Доступ к информации, распространяемой посредством информационно-телекоммуникационных сетей, в том числе сети “Интернет”, в местах, доступных для детей, предоставляется лицом, организующим доступ к сети “Интернет” в таких местах (за исключением операторов связи, оказывающих эти услуги связи на основании договоров об оказании услуг связи, заключенных в письменной форме), другим лицам при условии применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от информации, причиняющей вред их здоровью и (или) развитию.

ПУНКТ 24-1 ПОСТАНОВЛЕНИЯ

В случае заключения срочного договора об оказании разовых услуг по передаче данных в пунктах коллективного доступа оператор связи осуществляет идентификацию пользователей и используемого ими оконечного оборудования.

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

А это значит, что теперь заходя в кафешку (или другое публичное место) с призывной надписью «WiFi FREE» - готовьте паспорт… ну или мобильный телефон для получения смс с кодом доступа от Вашего оператора. Еще один вариант входа в интернет в «пункте коллективного доступа» – наличие регистрации на Портале государственных услуг (http://gosuslugi.ru), но пока известен только один оператор, предоставляющий доступ в интернет таким способом.

УГОЛОВНЫЙ КОДЕКС РОССИЙСКОЙ ФЕДЕРАЦИИ

ОСНОВНЫЕ МОМЕНТЫ:

СТАТЬЯ 272. НЕПРАВОМЕРНЫЙ ДОСТУП К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, в зависимости от его тяжести наказывается либо штрафом, либо лишением свободы.

СТАТЬЯ 273. СОЗДАНИЕ, ИСПОЛЬЗОВАНИЕ И РАСПРОСТРАНЕНИЕ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ.

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, в зависимости от тяжести наказываются либо ограничением, либо принудительными работами, либо лишением свободы.

СТАТЬЯ 274. НАРУШЕНИЕ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, в зависимости от тяжести наказывается либо штрафом, либо принудительными работами, либо лишением свободы.

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

Ну собственно это значит, что лазить на чужой компьютер без разрешения хозяина нельзя! Нельзя красть от туда информацию, удалять её, менять по своему усмотрению и т.д. Нельзя создавать и распространять компьютерные вирусы и другие «зловредные» программы, мешающие работе компьютеров интернет-пользователей!

А тем, кто работает с компьютерами и другой умной электроникой ИТ-оборудованием нельзя нарушать инструкции и правила эксплуатации такой техники, составленные работодателем.
Все эти действия могут повлечь большие неприятности.

ПРАВИЛА ПРОДАЖИ ТОВАРОВ ДИСТАНЦИОННЫМ СПОСОБОМ УТВЕРЖДЕНЫ ПОСТАНОВЛЕНИЕМ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 27.09.2007 Г. № 612

ОСНОВНЫЕ МОМЕНТЫ:

ПУНКТ 5

Не допускается продажа дистанционным способом алкогольной продукции, а также товаров, свободная реализация которых запрещена или ограничена законодательством Российской Федерации

ЧТО ЭТО ЗНАЧИТ ДЛЯ НАС С ВАМИ?

Именно то, что написано – не надо пытаться продать через интернет то, что вообще нельзя продавать, а также алкоголь.

Резюмируя данный раздел хочется сказать, что если кто-то говорит Вам, что «в интернете можно всё», не верьте! Интернет – это такая же часть нашей жизни, здесь работают такие же законы, и если в оффлайне нельзя красть, обманывать и продавать отраву, то и в интернете этого делать нельзя. И, как известно, наши бдительные правоохранительные органы «все время на посту», хотя «наш суд – самый гуманный суд в мире».

ТУТ ВАМ МОГУТ ПОМОЧЬ (ПОЛЕЗНЫЕ ССЫЛКИ):

МВД РОССИИ
HTTPS://MVD.RU/

В принципе в полицию можно обращаться по фактам большинства видов преступлений, а Управление «К» МВД России (https://mvd.ru/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii) так специально создано для расследования «преступлений в сфере компьютерной информации».

Через сайт МВД можно отправить электронное обращение, но помните, что именно заявления о происшествиях или преступлениях принимаются только лично от граждан в дежурных частях территориальных органов внутренних дел и по телефону 02 (112 для мобильных телефонов).

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ (РОСКОМНАДЗОР)
HTTP://RKN.GOV.RU/

Сюда надо обращаться в случае, если Вы обнаружили нарушение Ваших прав в части обработки персональных данных.

Кроме того, Роскомнадзор ведет:

- «Единый реестр доменных имен, указателей страниц сайтов в сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено» (http://eais.rkn.gov.ru/),
- «Реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка» (http://398-fz.rkn.gov.ru/),
- «Реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространяемую с нарушением авторских и (или) смежных прав» (http://nap.rkn.gov.ru/)
- «Реестр организаторов распространения информации в сети “Интернет” и сайтов и (или) страниц сайтов в сети “Интернет”, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети “Интернет”» (http://97-fz.rkn.gov.ru/), а значит туда можно обращаться также в случаях обнаружения в Сети информации, нарушающей законодательство Российской Федерации (ну или

если вдруг Ваш сайт/блог внезапно и без технических на то подоплёк стал недоступен пользователям).

Ну и сюда же можно обращаться по вопросам нарушения законодательства РФ в сфере средств массовой информации.
Очень удобно, что Роскомнадзор принимает обращения в электронном виде.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ ЗАЩИТЫ ПРАВ ПОТРЕБИТЕЛЕЙ И БЛАГОПОЛУЧИЯ ЧЕЛОВЕКА (РОСПОТРЕБНАДЗОР)

HTTP://ROSPOTREBNADZOR.RU/

Как видно из названия Роспотребнадзор выполняет функции по защите прав потребителей, а это значит, что обращаться сюда можно в случаях нарушения Ваших прав со стороны российских интернет-магазинов.
Приём обращений в электронном виде, осуществляется.

КООРДИНАЦИОННЫЙ ЦЕНТР НАЦИОНАЛЬНОГО ДОМЕНА СЕТИ ИНТЕРНЕТ

HTTP://CCTLD.RU/RU/

Координационный центр является администратором российских доменов верхнего уровня «.RU» и «.РФ». Сюда имеет смысл обращаться, если Вы столкнулись с проблемами в части использования доменных имен с окончаниями .ru и .рф. Сотрудники Координационного центра не занимаются расследованием преступлений, но могут подсказать как действовать в той или иной ситуации.
Ну и вполне естественно, что администратор российских национальных доменов принимает обращения в электронном виде (хотя и не чужд использования исконных способов переписки в бумажном виде).

ГОРЯЧАЯ ЛИНИЯ ЛИГИ БЕЗОПАСНОГО ИНТЕРНЕТА

HTTP://HOTLINE.FRIENDLYRUNET.RU/?L=RU

Горячая линия принимает сообщения о распространении в сети интернет материалов с порнографическими изображениями несовершеннолетних.
Обратиться сюда можно по телефону +7 (499) 685–01–85, по электронной почте info@FriendlyRunet.ru или через сайт.

ГОРЯЧАЯ ЛИНИЯ ГРУППЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (GROUP-IB)

HTTP://WWW.CERT-GIB.RU/REPORT.PHP

По соглашению с Координационным центром национального домена сети интернет Group-IB занимается противодействии киберугрозам в доменах .РФ и .RU. Так что если Вы обнаружили, что доменное имя используется в целях

фишинга, несанкционированного доступа в информационные системы третьих лиц, распространения вредоносных программ и управления вредоносными программами (бот-сетями) – Вам сюда.
Обращения принимаются круглосуточно по телефону +7 (495) 988-00-40, по электронной почте response@cert-gib.ru или через сайт.

ГОРЯЧАЯ ЛИНИЯ ЛАБОРАТОРИИ КАСПЕРСКОГО

HTTP://NEWVIRUS.KASPERSKY.RU/

Лаборатория Касперского традиционно занимается фактами распространения в Сети компьютерных вирусов.
Обратиться в Лабораторию за помощью Вы можете как в электронном виде (по электронной почте cert@kaspersky.com или через сайт, так и по бесплатному телефону +7 (800) 700-88-11.

ЛИНИЯ ПОМОЩИ «ДЕТИ ОНЛАЙН»

HTTP://DETIONLINE.COM/HELPLINE/ABOUT

Линия помощи «Дети онлайн» — бесплатная всероссийская служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования интернета и мобильной связи.
Обращения принимаются по бесплатному телефону 8-800-25-000-15 или через форму обратной связи на сайте.

ГОРЯЧАЯ ЛИНИЯ РОЦИТ (РЕГИОНАЛЬНАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ «ЦЕНТР ИНТЕРНЕТ-ТЕХНОЛОГИЙ»)

HTTP://WWW.HOTLINE.ROCIT.RU/

На горячую линию можно сообщить о контенте, который, по Вашему мнению, нарушает российское законодательство, а также сообщить о проблемах, связанных с предоставлением тех или иных услуг в интернете (нелегальные/противоправные материалы, мошенничество, проблема с интернет-сервисом (интернет-банкинг, интернет-магазин и пр.), низкое качество интернет-услуг).

АДМИНИСТРАЦИИ САЙТОВ

Большинство сайтов в интернете все же создано не для обмана пользователей и администрации, как правило, заинтересованы в том, чтобы удержать пользователя на своем сайте. Поэтому в случае возникновения каких-либо проблем с сайтом или подозрения на обман/мошенничество со стороны другого пользователя сайта, не стесняясь пишите в форму обратной связи ресурса.

СЛОВАРЬ ТЕРМИНОВ, ИСПОЛЬЗОВАННЫХ (И НЕ ИСПОЛЬЗОВАННЫХ) В ТЕКСТЕ

Анонимайзер – техническое или программное средство для скрытия информации о компьютере или пользователе в интернете.

Антивирус (антивирусная программа) – специальная программа, предназначенная для защиты Вашего компьютера от различных «вирусов».

Бот (сокращение от «робот») – компьютер, зараженный специальной программой (вирусом), позволяющей злоумышленнику управлять таким компьютером по своему усмотрению без согласия владельца компьютера. Из «бот-компьютеров» создаются «бот-сети» («бот-неты»), занимающиеся, например, рассылкой спама или атакой на ресурсы банков, и все это при полном неведении хозяев таких компьютеров.

Вирус (компьютерный вирус) – программа, установленная на компьютер пользователя без его ведома с целью получить доступ к информации, хранимой на компьютере (файлам, паролям и т.д.) или ресурсам компьютера пользователя.

Доменное имя – имя сайта, которое Вы видите (или набираете) в строке браузера (например «yandex.ru» или «президент.рф»).

Интернет-тролль – пользователь Сети интернет, занимающийся троллингом, то есть человек, который своими комментариями пытается вывести другого пользователя из состояния душевного равновесия (в основном – разозлить или расстроить).

Интернет-форум (форум) – интернет-площадка (сайт), созданная для обсуждения какого-то конкретного вопроса, и являющиеся более узким вариантом социальной сети, – позволяют быстро найти или услышать ответы на интересующие вопросы.

Контент – обобщенное название всего того, что можно скачать (посмотреть, почитать, послушать и т.д.) в интернете (программы, тексты, фильмы и др.).

Мессенджеры – программы для мгновенного обмена сообщениями.

Модератор – пользователь форума или сайта, имеющий право редактировать и удалять сообщения других пользователей и даже удалять или блокировать самих пользователей, нарушающих правила сайта.

Нигерийские письма (или иначе «письма счастья») – вид электронных писем, распространяемых мошенниками с целью выманить у интернет-пользователя максимально возможную сумму денег. Отличительной чертой таких писем, является то, что в их начале содержится текст о «свалившихся на голову» адресату несметных богатствах (большом наследстве, выигрыше или т.д.), для получения которых пользователь должен перевести некоторую денежную сумму. Зачастую пишутся они далеко за границей и отправляются в Россию с автопереводом, поэтому не отличаются складностью и красотой звучания русского языка. «Нигерийскими» такие письма были названы потому, что зародился этот вид мошенничества именно в Нигерии.

Ник или никнейм/никнэйм (от английского «nickname» – «кличка» или «прозвище») – сетевое имя или псевдоним интернет-пользователя.

Онлайн – в интернете.

Оффлайн – вне интернета.

Пост – отдельное сообщение в блоге или форуме.

Социальная сеть – сайт, созданный с целью собрать на одной интернет-площадке людей с общими интересами (живущих в одном городе, учившихся когда-то вместе, интересующихся одним стилем музыки или артистом, и т.д.), дать им возможность общаться на различные темы, добавлять друг друга в друзья, выкладывать и обсуждать фотографии и видео…

Спам – рассылка электронных писем (чаще рекламы) людям, не выражавшим желания их получать.

Торрент – система передачи файлов (файлового обмена между пользователями) с использованием специального программного обеспечения. Особенность этой системы в том, что файлы передаются частями с компьютеров пользователей уже скачавших файл, при этом скорость закачки напрямую зависит от количества таких компьютеров. После закачки всех частей файла торрент-программа (торрент-трекер) собирает его в одно целое.

Троллинг – агрессивные, оскорбительные или провокационные комментарии в социальных сетях, призванные обидеть или разозлить автора «поста».

Троян («троянская программа», «троянский вирус») – вид вредоносной программы (компьютерного вируса), скрывающейся внутри другой программы (по аналогии с легендарным троянским конем).

Файлообменник – это сервис, на котором пользователь может разместить свой файл (или несколько файлов) в интернете, а взамен получить ссылку (гиперссылку), по которой этот файл будет круглосуточно доступен всем, кому она будет известна.

Фейк (от английского «fake» – подделка, фальсификация, подлог, обман) – специально сделанная ложная информация, зачастую трудноотличимая от правды.

Фишинг (от английского «fishing» – рыбная ловля, выуживание) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям.

Флуд (от английского «flood» – «потоп») – размещение в социальных сетях, чатах и форумах не тематических сообщений или большого количества однородной информации и бессмысленных символов, зачастую занимающие большие объёмы.

Электронный адрес (адрес электронной почты, E-mail) – выглядит как: имя пользователя (он же логин), которое пользователь придумывает сам, символ @ («собака»), имя сервера, на котором находится почтовый ящик, точка и буквенное обозначение домена. Например, my@company.ru.