Глава 2

# Безопасен ли Интернет? Вирусы, программы-шпионы, спам и прочая гадость

*В этой главе...*

- ✓ Кто есть кто и что посторонние могут узнать о вас
- ✓ С кем я общаюсь
- ✓ Как посторонние могут получить контроль над вашим ПК
- ✓ Спам
- ✓ Какое секретное слово вы знаете, мистер Поттер?
- ✓ Позаботьтесь о безопасности — своей собственной и близких

Мы любим Интернет, он стал частью нашей жизни — и способом заработать на жизнь — еще много лет назад. Мы были бы рады сказать вам, что многочисленные сообщения о том, что подключать компьютер к Интернету опасно, — чепуха. Но не можем сделать это. Популярность "Всемирной паутины" привлекла в нее множество людей, которые относятся к вам как к денежному дереву, мечтающему о том, чтобы его как следует ободрали. (Ничего личного. Они ко всем так относятся, не только к вам.) В некоторых странах мошенничество в Интернете стало важной частью национальной экономики.

Даже если никто не будет красть ваши деньги, информация о поведении в Интернете может считаться покушением на конфиденциальность личной жизни. Существует порода людей, которые пытаются получить контроль над вашим компьютером, чтобы использовать его в неблаговидных целях. Как только очередной компьютер подключается к Интернету, возникает вопрос не о том, будет ли он подвергнут кибератаке, а о том, как скоро это произойдет. И произойдет это не через месяцы или дни, но через считанные часы или даже минуты.

И все же не переживайте — Интернет нельзя отнести к опасным местам. Вы рискуете не больше, чем во время прогулки по большому городу. Да, вы должны быть осторожными, соблюдать определенные правила безопасности и не забредать в районы с сомнительной репутацией, но вместе с тем вы можете, ничем особенно не рискуя, воспользоваться всеми преимуществами, предоставляемыми Интернетом.

В этой главе описываются проблемы конфиденциальности, безопасности и надоедливости, в изобилии встречающиеся при работе в Интернете.

- ✓ Проблемы конфиденциальности связаны главным образом с тем, как много посторонних могут узнать о вас через Интернет.
- ✓ Проблемы безопасности — как сохранить полный контроль над программами, выполняемыми на вашем компьютере.

- ✓ Проблемы надоедливости — как избавиться от многочисленных писем со всевозможными предложениями, переполняющими ваш ящик электронной почты (они получили название *спам*), и от всплывающих окон с рекламой, мешающих просматривать веб-страницы.

В оставшейся части книги мы дадим инструкции по обеспечению безопасности за счет использования брандмауэра, антивирусного программного обеспечения, сканеров программ-шпионов и просто здравого смысла. В главе 3 говорится о правилах, которые должны соблюдать дети, имеющие доступ к Интернету; они справедливы и для большинства взрослых.

# Кто есть кто и что посторонние могут узнать о вас

Преимущества новых технологий заставляют пересмотреть понятия о гарантированном праве на "личную жизнь". Инновации, которыми мы пользуемся ежедневно, — платежные и дисконт-карты, мобильные телефоны, электронные ключи и автомобильные радиостанции, — позволяют отследить каждую нашу покупку, каждое передвижение. Интернет лишь усугубил эту тенденцию. Большая часть из того, чем вы занимаетесь в онлайновом режиме, может быть выявлена и зафиксирована — иногда без злого умысла, иногда с таковым.

Все это усугубляется степенью общедоступности личной информации, которая становится еще более открытой благодаря Интернету. Когда документы хранились в правительственных учреждениях и тот, кому была нужна информация личного характера, должен был явиться в это учреждение и убедить служащих поискать ее в файлах, злоупотреблений было намного меньше. Современные технологии позволяют кому угодно и откуда угодно получить доступ к информации о дотоле совершенно неизвестном ему человеке и накопить информацию, полученную из разных источников, в том числе из Интернет-каталогов. Никого теперь не могут защитить ни расстояние, ни время.

Некоторых людей беспокоит то, что через Интернет кто-то может подсмотреть их частную переписку по электронной почте и отследить веб-страницы, которые они просматривают. На самом деле это маловероятно. Более серьезная проблема — рекламодательные компании, которые создают ваш "профиль" на основе сайтов, которые вы посещаете, и товаров, которые приобретаете. Эта информация затем используется для целенаправленной рекламы. Наиболее известные компании такого рода отрицают, что создают персональные профили, но не обещают не делать этого в будущем.

Несколько способов сбора информации о вас в то время, когда вы пользуетесь Интернетом, или подсовывания потенциально опасной для вас информации описаны в следующих разделах.

## С кем я общаюсь

Кажется, что "Всемирная паутина" абсолютно анонимна, хотя на самом деле это не так. Раньше пользователи получали имена в Интернете, которые хоть как-то напоминали их собственные данные, — имя, инициалы или некоторую их комбинацию в сочетании с названием университета или корпорации. Это давало возможность перекинуть мостик к реальной личности пользователя. Сейчас создание нового адреса электронной почты занимает всего лишь несколько минут, и приоткрывать завесу над тайной своей реальной личности стало совершенно необязательным.

В зависимости от того, кто вы и что собираетесь делать в Интернете, вы можете иметь несколько имен и адресов, причин может быть несколько, например.

- ✓ Вы — профессионал (например, физик) и хотите воспользоваться списками рассылки или группами новостей, но так, чтобы никто не интересовался вашим профессиональным мнением.
- ✓ Вы ищете помощи в чем-то, что считаете весьма конфиденциальным, и не хотите, чтобы эти проблемы стали известны близким людям, которые могут узнать вас по ассоциации с электронным именем.
- ✓ Вы ведете бизнес с помощью "Всемирной паутины" и одновременно активно общаетесь через Интернет. Тогда вам, возможно, захочется отделить одно занятие от другого.


Большинство ваших действий в Интернете можно проследить. Те, кто злоупотребляют своей анонимностью во "Всемирной паутине", могут вдруг обнаружить, что она не так уж и абсолютна.

## Безопасность превыше всего

Анонимность, бесценное качество Интернета, имеет и обратную сторону. Чтобы обезопасить себя и свою семью, придерживайтесь следующих простых правил.

- ✓ В комнатах для бесед (чатах) и в других аналогичных ситуациях не пользуйтесь своим полным именем.
- ✓ Никогда не сообщайте свое имя, адрес или номер телефона человеку, которого вы не знаете.
- ✓ Не доверяйте человеку, который представляется вам работником службы технической поддержки или сотрудником аукциона *eBay* и просит сообщить ему ваш пароль. Ни один легитимный сотрудник подобной службы никогда не будет интересоваться вашим паролем.
- ✓ Будьте особенно осторожны, сообщая информацию о своих детях. При посещении комнат для бесед не заполняйте формы, в которых запрашивается имя, место проживания, возраст, название школы, номер телефона ваших детей. Такая информация очень часто используется для "целевого маркетинга" (читай: для рассылки "макулатурной" почты).

Иногда (правда, достаточно редко) с людьми, которые переносили свои знакомства из Интернета в реальную жизнь, случались весьма неприятные вещи. Однако чаще все же бывает наоборот. Мы познакомились через Интернет со многими из наших лучших друзей, а некоторые наши знакомые, познакомившись через Интернет, поженились. Руководствуйтесь здравым смыслом, когда назначаете встречу со своим сетевым другом. Человек, с которым вы переписывались электронной почтой или познакомились через систему мгновенного обмена сообщениями, все еще остается для вас посторонним, поэтому примите те же предосторожности, которые обычно принимаете при встрече с малознакомыми людьми: назначьте встречу в людном месте, придите на нее с другом и позаботьтесь о том, чтобы ваша семья знала, где вы и когда планируете вернуться.

Интернет — прекрасное место, а возможность встречаться с людьми и заводить новых друзей — одно из самых ценных его свойств. Но будьте здесь также внимательны и предусмотрительны, как и в обычной, "реальной" жизни.

## Фишинг ради информации

Фишинг (от англ. *phishing*) — это быстро распространяющийся способ мошенничества в Интернете, и вы можете стать его жертвой. Хорошая новость состоит в том, что защититься от этой напасти можно очень просто, если только вы и члены вашей семьи знают, что нужно делать, чтобы не попасться на крючок.

### *На что похож фишинг?*

На ловлю рыбы. Наживка может быть разной. После того как вы начнете пользоваться Интернетом и получать электронную почту (как описано в главе 12), велика вероятность того, что вам придет сообщение о том, что кто-то использует вашу учетную запись при участии в онлайновых аукционах. Чтобы уберечь вас от неприятностей, в письме будет предложено ввести определенный код в форму, ссылка на веб-страницу с которой приводится в этом же письме ниже. Она, например, может выглядеть так:

```
http://www.eBay.com/cgi_bin/secure/Fraud Alert ID CODE: 00937614
```

т.е. в точности как та, к которой вы, возможно, уже обращались (за исключением добавленного кода). В форме, открывающейся после щелчка на ссылке, будет предложено повторно указать ваши регистрационные данные, иначе ваша регистрация будет аннулирована в течение 48 часов.

Щелкнув на ссылке, вы действительно попадете на уже знакомую (возможно) вам страницу, где когда-то регистрировались. Вы можете повторить эту процедуру — и попадетесь на удочку, потому что эта веб-страница — подставная. Как только вы введете свои имя пользователя и пароль, откроется другая страница, на которой предложат ввести номер кредитной карточки, PIN, адрес, по которому можно выслать счет, состояние вашего текущего счета, дату рождения, девичью фамилию матери, номер водительских прав. Эта форма достаточно "умна" для того, чтобы отвергнуть недействительный номер кредитной карточки. После того как вы введете все эти данные и щелкнете на кнопке Далее, откроется настоящая страница онлайнового аукциона с сообщением о том, что вы вышли из системы. А потом — кто знает? Вы теперь открыты для всего — от совершения мелких покупок по вашей кредитной карточке до полномасштабной подмены вашей личности, на борьбу с чем уйдут месяцы или даже годы.

Это сообщение пришло, конечно, не от владельцев онлайнового аукциона. Миллионы подобных сообщений от имени всемирно известного аукциона *eBay* ежедневно рассылаются электронной почтой. Знатоки английского языка могут заподозрить неладное, проанализировав тест сообщения. В нем, например, могут встретиться слова с ошибками, типа *recieved* и *informations*, указывающие на то, что автор письма плохо знает английский. Но надежнее всего — сохранить полученное сообщение электронной почты в виде файла и распечатать его, после чего выяснится, что вполне правдоподобная ссылка на сайт аукциона eBay представляет собой на самом деле лишь часть полной ссылки, которая может быть такой:

```
<http://192.168.45.67/cgi_bin>http://www.eBay.com/cgi_bin/secure/
Fraud Alert ID CODE: 00937614
```

Текст, заключенный между угловыми скобками (< и >), — это реально действующая ссылка на "подставной" сайт, адрес которого указан цифрами. (Когда мы попытались перейти по этой ссылке два дня спустя, получили сообщение, что этот сайт уже ликвидирован. Видимо, "подсуетилась" служба безопасности аукциона *eBay*.)

### *Не хватайте приманку*

Рано или поздно "рыбаки" перестанут делать ошибки в письмах или найдут хороших редакторов, так что их письма нельзя будет отличить столь простым способом. Дадим еще несколько советов.

- ✓ Считайте, что любое полученное сообщение электронной почты с предложением открыть страницу, на которой от вас потребуют сообщить пароль, номер кредитной карточки или другую информацию личного характера, — это попытка фишинга.
- ✓ Если в сообщении идет речь о компании, с которой вы раньше не имели никаких дел, уничтожьте его.
- ✓ Если речь идет о компании, в которой у вас открыт счет, зайдите на сайт компании, введя ее URL в строке адреса вашего браузера (глава 7), но *ни в коем случае* не щелкайте на ссылке, указанной в письме. На сайте компании поищите ссылку типа My account (Мой счет). Если вы зарегистрированы на этом сайте и действительно возникли какие-то проблемы, вы найдете соответствующее примечание. Если вы не зарегистрированы или не можете зарегистрироваться, но вас по-прежнему волнует полученное сообщение, перешлите его копию в отдел по работе с клиентами.

Один из трюков, используемых "рыбаками" против начинающих пользователей Интернета, называется *спуфинг сайта* (*site spoofing*): они вынуждают ваш браузер отображать адрес одного сайта, в то время как на самом деле вы просматриваете страницу другого. Некоторые браузеры позволяют веб-сайтам отображать только его основной адрес, чтобы он не выглядел так устрашающе. Именно этим и пользуются "рыбаки". Хорошие браузеры, такие как Firefox (глава 6), обеспечивают защиту от спуфинга — они всегда отображают настоящий адрес страницы, которую вы просматриваете.

**Вывод.** Члены вашей семьи должны запомнить: никогда, *никогда*, **никогда** не следует вводить пароль, номер кредитной карточки или иную информацию личного характера на веб-странице, которая была открыта щелчком на ссылке в электронном письме.

## Веб-маяки и жучки, отслеживающие посещения сайтов

С тех пор как выражение World Wide Web стало обиходным для миллионов людей, компании все чаще рассматривают свое присутствие в Интернете как жизненно важный для них способ рекламировать свои товары и услуги и продвигать бизнес. Они тратят миллионы долларов на свои веб-сайты и очень хотели бы знать, как люди пользуются ими. Поэтому нет ничего удивительного в том, что, как только вы заходите на такой сайт, компании начинают отслеживать ваши перемещения и переходы от одной ссылки к другой в пределах их сайта. Но гораздо важнее им знать, чем вы занимались до того, как посетили их сайт, и чем будете заниматься после того, как уйдете с него. Для того чтобы получить эту информацию, они используют особые фрагменты кода, называемые *веб-маяками* (Web beacons) или *веб-жучками* (Web bugs), которые сообщают о вашем поведении на центральный сайт, часто принадлежащий отдельной компании, занимающейся рекламой в Интернете. Обрабатывая информацию, полученную со многих сайтов, такие "следящие" компании могут получить полное представление о том, чем вы занимаетесь во "Всемирной паутине" и что вы в ней в ищете.

Многие такие компании собирают только статистическую информацию для своих клиентов, но потенциал ее использования с другими целями сохраняется. Нельзя не отметить тот факт, что американские суды установили более низкий стандарт по защите от такой "регистрации деловых операций", чем таковой по защите личных документов, хранящихся в вашем доме.

## Файлы "cookie" — это не так уж плохо

Когда вы просматриваете веб-страницы (об этом более подробно сказано в главе 6), веб-сервер должен знать, кто вы, если вы собираетесь зарегистрироваться на нем, или положить какой-то товар в виртуальную тележку для покупок, или сделать еще что-то такое, для чего веб-сайту нужно запоминать информацию о вас на то время, пока вы переходите с одной его

страницы на другую. Наиболее часто используемый способ отслеживания ваших действий на веб-сайте называется *установка файлов "cookie"*. Это — крошечные файлы, сохраняемые на вашем компьютере. Каждый из них содержит адрес веб-сайта и программный код, каким-либо образом идентифицирующий вас. Файлы "cookie" обычно не содержат какую-либо персональную информацию и вообще не опасны, они безобидны и полезны.

**Ваш Google**

Одной из главных привлекательных черт Интернета является легкий доступ к *любым* данным. Некоторые из этих данных могут относиться к вам. Если у вас есть свой персональный сайт или вы ведете сетевой дневник (главы 16 и 17), вы можете рассчитывать на то, что размещенная вами в Интернете информация окажется доступной для других, обычно для всех, желающих с нею познакомиться. (Мы все еще находим в Интернете свои высказывания, сделанные 25 лет назад.) Но другие люди также размещают в Интернете информацию — статьи, сообщения о всевозможных событиях, свои фотографии, другие фото и т.п. Шлейф оставленных вами в Интернете электронных данных может оказаться длиннее, чем вы думаете. Если вы еще не сделали это, попробуйте поискать их с помощью Google. Введите свое имя в кавычках в поле ввода слов запроса поисковой системы Google и щелкните на кнопке Go (Найти). Если ваше имя относится к числу распространенных, введите еще инициал отчества (или второго имени) или добавьте название вашего города либо школы, которую вы закончили. Если вы будете заниматься этим все время, то знайте, подобная мания называется *эгосерфинг* (поиск упоминаний собственного имени в WWW, базах данных, результатах исследований, печатных изданиях и т.д.).

Если вы планируете совершать покупки в интернет-магазинах (об этом рассказывается в главе 10) или пользоваться многими другими службами Интернета, знайте: все это можно делать благодаря файлам "cookie". Например, когда вы резервируете место на авиарейс, соответствующий сайт использует технологию "cookie" для того, чтобы сохранить это место за вами и не позволить другим потенциальным пассажирам "занять" его, пока вы не закончите процедуру заказа.

С другой стороны, представьте, что вы воспользовались кредитной карточкой для покупки какого-нибудь товара в интернет-магазине. Веб-сайт магазина воспользовался файлом "cookie" для того, чтобы "запомнить" номер вашей кредитной карты. Если вы совершили покупку со своего служебного компьютера, то и другой человек может с того же компьютера посетить тот же интернет-магазин. Возможно, он даже сможет оформить покупку по вашей кредитной карточке. Приплыли!

Пользователи Интернета по-разному относятся к файлам "cookie". Некоторые не обращают на них внимания, другие считают неоправданным вмешательством в личную жизнь. Вы должны сами решить, как к ним относиться. Вопреки слухам, файлы "cookie" не способны получать информацию, содержащуюся на жестком диске вашего компьютера, снимать с вашего счета деньги и вмешиваться в вашу жизнь. Они просто собирают информацию, полученную от браузера. А такие их (браузеров) разновидности, как Internet Explorer и Firefox, позволяют контролировать, где и когда файлы "cookie" сохраняются на вашем компьютере. В главе 7 подробно рассказано о том, как, где и когда можно позволить вашему браузеру устанавливать файлы "cookie".

# Как посторонние могут захватить контроль над вашим ПК

Вы загружаете из Интернета и устанавливаете на свой компьютер какую-то полезную программу. Это замечательно, когда вы можете воспользоваться утилитой просмотра и распечаткой декларации для налоговой инспекции или когда устанавливаете обновлен-

ную версию программы, купленной прежде. Это очень удобно! Мы еще вернемся к этому вопросу в главе 11.

Однако есть и другой вариант: кто-то посторонний может установить программу на ваш компьютер без вашего на то разрешения. Сразу же возникает вопрос: а кому принадлежит, собственно, компьютер?! Эти программы могут попасть на ваш компьютер различными путями, но чаще всего — через электронную почту и ваш браузер.

## Вирусы проникают через электронную почту

Компьютерные вирусы — это программы, которые передаются от одного компьютера к другому точно так же, как обычные вирусы передаются от человека к человеку. Компьютерные вирусы могут распространяться, используя такие механизмы передачи информации с одного компьютера на другой, как сети, компакт-диски с данными, DVD и даже ИК-лучи. Вирусы угрожают компьютерам уже длительное время. На заре своего существования вирусы содержались в файлах, которые пользователи загружали на свои компьютеры с помощью протоколов передачи файлов или веб-браузеров. В наше время большая часть вирусов распространяется через файлы, пересылаемые электронной почтой в виде приложений к письмам, а также в системах мгновенной передачи сообщений (о которых будет говориться в главе 15), причем последний способ применяется все чаще.

Было время, когда знающие люди (к которым мы относили и себя) смеялись над новичками, которые боялись заразить свой компьютер вирусом через электронную почту. Электронные письма были просто текстовыми файлами и не могли содержать программ. Но потом появились вложения в электронные письма. Пользователи получили возможность посылать друг другу программы — в том числе содержащие вирусы — через электронную почту. Прогресс — замечательная вещь, не правда ли?

### *Что делают вирусы?*

Когда вирус попадает на компьютер, он должен каким-то образом быть выполненным. *Быть выполненным* на компьютерном сленге означает быть пробужденным к жизни. Вирус представляет собой программу, а всякая программа должна быть выполнена, для этого она должна быть “включена”, “запущена” или “начата”. Будучи запущенным, вирус делает две вещи.

1. Вначале он “осматривается” и пытается найти вашу адресную книгу, которую использует для того, чтобы разослать самого себя всем вашим друзьям и знакомым, часто прикидываясь весьма убедительным предложением (“Эй, давай повеселимся следующей ночью, этот файл поможет нам!”).
2. Затем он выполняет свою миссию — делает то, для чего был написан своим создателем, который ради этого рискует попасть за решетку (что чаще всего и случается).

Миссия заключается в незаконной деятельности, осуществляемой вирусом на вашей машине. Это может быть, например, запись каждого нажатия клавиши (в том числе при вводе пароля). Это может быть атака через ваш компьютер на определенный или случайный сайт Интернета. Это может быть рассылка спама с вашего компьютера. Как бы там ни было, это не то, чего вы ждете от электронного помощника. Поверьте. Если ваш компьютер начинает вести себя странно или резко сбавляет темп, скорее всего, причина в том, что вы подцепили вирус — или два десятка вирусов.

В старое доброе время вирусописатели занимались этим лишь ради того, чтобы узнать, как быстро распространяются вирусы, но, как во всем, что связано с Интернетом, создание вирусов стало крупным бизнесом, во многих случаях контролируемым преступными синдикатами.

### Какое средство годится против вирусов?

Не беспокойтесь особенно насчет вирусов. Существует множество антивирусных программ, которые проверяют все сообщения, поступающие с электронной почтой, еще до того, как вирус сможет начать атаку. В главе 4, в которой описывается процедура подключения к Интернету, мы рекомендуем установить антивирусную программу. После того как вы ее установите, не забывайте регулярно обновлять свою антивирусную программу, чтобы она могла защищать компьютер от новых вирусов.

## Червяки приползают через Интернет

*Червь* похож на вирус, но он распространяется безадресно, в отличие от электронной почты. Он просто переходит с одного компьютера на другой через Интернет, используя скрытые ошибки в программном обеспечении. К сожалению, большая часть популярного программного обеспечения, предназначенного для обслуживания работы "Всемирной паутины", начиная с Microsoft Windows, изобилует скрытыми "дырами", поэтому, как только вы подключите свой новый замечательный компьютер с системой Windows к Интернету через широкополосное соединение, он получит несколько червей в течение первой же минуты.

Если вы тщательно следите за обновлениями, предлагаемыми компанией Microsoft в плане защиты вашего компьютера, то большинство из выявленных "дыр" будет закрыто, но все же понадобится несколько минут, прежде чем это произойдет. Поэтому мы настоятельно рекомендуем всем, кто применяет широкополосное соединение с Интернетом, использовать аппаратный брандмауэр — "ящик", устанавливаемый между сетью и компьютером и предохраняющий его от нашествия червей. Если вы применяете широкополосное соединение, то, возможно, захотите использовать недорогое устройство, называемое *маршрутизатор*, для подключения компьютера к чему угодно; все маршрутизаторы содержат брандмауэры в качестве стандартного устройства. (Более подробно об этом сказано в главе 4.)

## Шпионские программы поступают с веб-сайтов

Шпионские программы (в том числе распространяющие рекламу) похожи на вирусы, но они используют ваш компьютер с иной целью. Их распространение осуществляется не через электронную почту, загрузка осуществляется через браузер. В самом общем случае вы должны щелкнуть на каком-либо объекте, расположенном на веб-странице, после чего на ваш компьютер будет установлена шпионская программа. Однако большинство пользователей легко поддаются соблазну установить шпионское ПО, при этом злоумышленники предлагают загрузить утилиту для просмотра изображений или другую полезную программу.

### Что делает шпионская программа

"Шпионским" программное обеспечение называется потому, что оно часто используется в таких неблаговидных целях, как отслеживание того, что вы набираете с помощью клавиатуры. Некоторые шпионские программы собирают вашу личную информацию и пересылают ее затем на какой-то сайт без вашего на то ведома и согласия. В общем случае шпионское программное обеспечение используется для того, чтобы выяснить, какие сайты вы посещаете, благодаря чему рекламодатели могут давать свои объявления во всплывающих окнах (о них рассказано ниже в данной главе) более целенаправленно, с учетом ваших интересов.

Целенаправленная реклама не является сама по себе злом. Например, программа Google AdSense позволяет рекламодателю размещать рекламные объявления, соответствующие содержанию найденных в процессе поиска системой Google страниц. Эффективность целенаправленной рекламы выше, чем обычной, потому что она в большей степени соответствует тому, что ищет пользователь.

Шпионское программное обеспечение может также рассылать спам с вашего компьютера, перехватывать каждое нажатие клавиши и пересылать информацию о нем злоумышленнику через Интернет, а также делать другие нехорошие вещи.

### *Не устанавливайте шпионское ПО добровольно*

Множество привлекательных программ можно загрузить на компьютер бесплатно, но не устанавливайте их на свой компьютер, пока не убедитесь в том, что они так же безопасны, как и полезны. Множество панелей инструментов, хранителей экрана и других утилит являются замаскированными шпионскими программами. Между прочим, чем больше программ запущено на вашем компьютере, тем медленнее они все работают. Посоветуйтесь с друзьями, прежде чем устанавливать новую программу. Или проведите поиск в Интернете по имени программы (глава 8), чтобы прочитать положительные и отрицательные отзывы о ней. Загружайте программы только с респектабельных сайтов.

### *Защищайте свой компьютер от шпионских программ*

Шпионские программы часто бывает трудно удалить — они могут внедриться в операционную систему компьютера. Не ждите, пока такая программа проникнет на ваш компьютер, чтобы затем заняться ее удалением; правильнее будет защитить его от заражения. Чтобы избежать этой неприятности, внимательно следите за тем, на каких ссылках вы щелкаете. И установите на свой компьютер программу, периодически сканирующую систему на предмет появления в ней шпионских программ. Более подробно об этом рассказано в главе 4.

**Бесплатные программы с рекламой — второе название шпионских программ**

Бесплатные программы с рекламой (adware) многими пользователями считаются также шпионскими, хотя это спорный вопрос. Вместе с бесплатно распространяемой программой устанавливается и ее часть, отвечающая за рекламу. Такие программы следят за тем, чем вы занимаетесь на своем компьютере, и отображают рекламные объявления — даже если вы в это время выполняете совсем другие программы. Противники бесплатных программ с рекламой считают, что ни один пользователь в здравом уме не станет устанавливать программу, которая будет досаждать ему рекламой, и они требуют законов, запрещающих такую практику, указывая, что бесплатные программы с рекламой часто ведут себя подобно паразитам, скрывая или подменяя собой рекламу конкурирующих сайтов.

Прежде чем загрузить бесплатную программу, убедитесь в том, что хорошо понимаете, что она будет делать. В противном случае не загружайте ее. Убедите ваших детей не загружать бесплатные игры, популярные песни и тому подобное. Большинство из них инфицировано рекламными программами, и прежде чем вы поймете это, на компьютер попадет столько рекламных объявлений, что придется “почистить” его, прежде чем вы сможете на нем работать.

## Всплывающие окна в браузере заслоняют все

Одно из наихудших изобретений последнего времени — всплывающие окна, которые неожиданно (для вас) появляются на экране компьютера при посещении некоторых веб-сайтов. Одни из них “выпрыгивают” мгновенно, другие прячутся под главным открытым окном и становятся видны только после его закрытия. Чаще всего с помощью всплывающих окон рекламируют ипотечные кредиты и авиабилеты. (Нет-нет, мы не собираемся называть эти фирмы поименно и тем самым рекламировать их.)

Появление всплывающих окон на вашем компьютере обеспечивается несколькими механизмами.

- ✓ Веб-сайт может открыть в вашем браузере новое окно. Иногда в этом окне отображается реклама или другая надоедливая информация. Но в некоторых случаях это

новое окно может содержать и полезную информацию — иные веб-сайты используют такие окна в качестве справочных, помогающих ориентироваться на сайте.

- ✓ Открывать всплывающие окна могут шпионские и другие программы.

К счастью, веб-браузеры сейчас обладают способностью не позволять сайтам открывать новые окна. О том, как научить браузер открывать поменьше всплывающих окон, рассказано в главе 7.

# Спам

Все чаще и чаще мы получаем непрошеные сообщения электронной почты от некоторых организаций или отдельных людей, с которыми мы не знакомы. Спам — это онлайновый эквивалент "макулатурной" почты. В реальной жизни те, кто рассылает рекламу почтой, должны оплачивать почтовые услуги. К несчастью, рассылка мириада сообщений через Интернет может практически ничего не стоить.

Рассылаемый электронной почтой *спам* — это тысячи копий нежелательных сообщений, посланных на адреса e-mail и даже через программы мгновенного обмена сообщениями.

Обычно такие сообщения содержат безвкусные рекламные объявления, описания методов быстрого обогащения или непристойные предложения сексуального характера, другими словами, то, что вы совсем не хотите читать и не хотите, чтобы это читали ваши дети. Такие сообщения называются *спамом*, практика рассылки этих сообщений — *спаммингом*, а человек, который их рассылает, — *спамером*. Многое из спама относится также к категории фишинга.

Спам стал большой проблемой в Интернете, потому что это действительно очень дешевый способ рекламы. Мы получаем сотни и тысячи ненужных писем каждый день, и их число продолжает расти. Спам бывает не только коммерческого, но и политического или религиозного содержания, главная его особенность заключается в том, что это всегда "незваный гость". Сообщение, которое вы хотите получить, спамом не является.

## Почему это называется "спам"

Это ветчина? Никто не знает фирмы, поставляющей ее. Ах, вы имеете в виду нежелательную электронную почту? Термин возник из телевизионных постановок группы *Monty Python*, в которых актеры, одетые в костюмы викингов, ни с того ни с сего начинали в темпе марша нараспев повторять слово *Spam*. (Проведите в Google поиск по запросу `Monty Python spam`, и вы найдете адреса множества сайтов, на которых можно почитать об этом.) Спам может "забить" ваш почтовый ящик настолько, что вы вообще перестанете им пользоваться.

Другая проблема — фильтры спама, которые предназначены для перехвата и удаления спама, но могут по ошибке удалить и полезные сообщения.

## Так ли это плохо

Может быть, вы думаете, что спам, подобно бумажной рекламной почте, не наносит никакого вреда и с ним вполне можно жить. Однако существует несколько отличий спама от бумажной рекламы, которую мы нередко находим в своем почтовом ящике. Первая из них — стоимость. В отличие от бумажной рекламы, вы, получатель, платите намного больше, чем отправитель спама. Отправка электронного сообщения — довольно дешевая услуга. Спамер со своего ПК с подключением через телефонную линию может разослать за час тысячи сообщений, а на загрузку этих сообщений вы теряете свое время и место на диске. После этого вы затрачиваете свое личное время на просмотр (по крайней мере темы сообщения) и их удаление. Количество спама уже превышает число полезных сообщений, и если количество спа-

ма будет продолжать разрастаться с такой тревожной скоростью, очень скоро электронная почта станет бесполезной, потому что нужные сообщения просто затеряются в потоке макулатуры. Другая проблема состоит в том, что фильтры спама, которые предназначены для отсеивания только спама, могут по ошибке отбросить и полезные для вас сообщения.

Спам поглощает не только ваши финансовые ресурсы, но и ресурсы почтовых серверов и всей "Всемирной паутины". Интернет-провайдеры взимают за его получение дополнительную плату со своих пользователей. По данным компании America Online, более чем 90% сообщений электронной почты, обрабатываемой этой компанией, представляют собой спам, а многие провайдеры сообщали нам, что от 2 до 20 долларов ежемесячной оплаты каждого пользователя приходится на обработку спама. Спамеры отсылают *100 миллиардов* сообщений *каждый день*. А когда провайдеры и компании начинают фильтровать почту, чтобы избавиться от спама, множество полезных писем ошибочно принимается за спам и не доставляется получателям.


Многие спам-сообщения, которые приходят пользователям, содержат инструкции о том, как отказаться от их получения. Это инструкции наподобие "пошлите нам сообщение, содержащее слово REMOVE". Не озадачивайтесь ответом, поскольку это — всего лишь способ удостовериться в том, что ваш адрес действующий; если вы пошлете такое сообщение, то получите *еще больше* спама. Отвечайте на сообщение или щелкайте на ссылке только в том случае, если письмо получено из списка рассылки, на который вы подписались, или от компании, с которой вас связывают деловые отношения.

## Что можно сделать

Вы не должны мириться со спамом. Фильтры спама способны оградить вас об большей части присылаемого спама. В главе 13 рассказано о том, как следует пользоваться фильтрами спама, встроенными в вашу почтовую программу, и как можно установить отдельную программу для фильтрации спама.

### Опасности бесплатных беспроводных подключений

Во многих общественных местах, от аэропортов до кафе, доступна услуга Wi-Fi — беспроводной способ подключения ноутбука к Интернету. В главе 4 рассказывается о том, как ваш компьютер можно подключить к Интернету через соединение Wi-Fi — вы находите сеть, щелкаете на кнопке Соединить (Connect) и начинаете работу в Интернете. Первое, что вы, вероятно, сделаете, — это воспользуетесь своим веб-браузером для получения электронной почты или подключения к сети компании, в которой работаете. И введете один-два пароля.

Можете ли вы доверять беспроводной сети? Уверены ли в том, что сеть не перехватывает нажатия клавиш, когда вы вводите пароль? Конечно, нет.

Спуфинг в сети Wi-Fi осуществляется на удивление легко. Злоумышленник устанавливает компьютер в холле аэропорта или в кафе, используя тот же самый идентификатор системы Wi-Fi, и вы подключаетесь к его компьютеру, а не к общедоступной сети. Он следит за тем, что вы набираете на клавиатуре, и использует ваши пароли для рассылки спама, опустошения вашего банковского счета и выполнения других мерзких действий.

Что должен делать путешествующий пользователь Интернета? Отвечаем: никогда не пользоваться бесплатной сетью Wi-Fi, пока вы не удостоверитесь в ее легальности. (Например, школа, в которой учатся ваши дети, или ваша компания могут развернуть сеть на территории школы или компании.) Если вам очень уж нужно воспользоваться общедоступной сетью Wi-Fi для получения электронной почты в пути, вот что нужно сделать (советы предоставлены нашим другом Марком Штайнвинтером).

1. Прежде чем отправляться в поездку, измените пароль электронной почты (и все другие пароли, которыми предполагаете воспользоваться).

2. Во время поездки ограничьте использование Wi-Fi, используйте только те учетные записи, пароли которых были изменены. Более того, не посещайте веб-сайты, которые требуют ввода пароля.
3. Тотчас по возвращении домой вновь измените пароли — на те, которые были раньше, или на другие. Имейте в виду, что плохим парням уже может быть известен пароль, которым вы пользовались во время поездки, поэтому никогда не используйте его впредь.

# Какое секретное слово вы знаете, мистер Поттер?

В наше время у вас повсюду спрашивают пароль либо какой-то код. Даже Гарри Поттер должен был сказать пароль волшебному портрету, чтобы пройти в спальню Гриффиндора. Эксперты по защите единогласны в рекомендациях относительно паролей.


- ✓ Используйте достаточно длинные и сложные пароли, чтобы никто не мог угадать их.

  Никогда не применяйте в качестве пароля слово, которое можно найти в словаре. Вставляйте в пароль одно-два числа.
- ✓ Никогда не используйте один и тот же пароль для разных учетных записей.
- ✓ Запоминайте пароль и нигде не записывайте его.
- ✓ Почаще изменяйте пароль.

**Будьте осторожны с подсказками для припоминания пароля**

Веб-сайтам надоело разбираться с клиентами, забывшими свой пароль, поэтому несколько лет назад появился новый вид услуг — подсказка пароля. Когда вы создаете новую учетную запись, дружественное программное обеспечение запрашивает у вас имя пользователя и пароль. При этом оно предлагает выбрать один ответ из нескольких, например “Какой ваш любимый цвет?” или “Как зовут вашу собаку?”

Через некоторое время вы попытаетесь зарегистрироваться на таком сайте и не сможете вспомнить пароль. Никаких проблем! Вам зададут секретный вопрос, который вы когда-то выбрали; если будет введен правильный ответ, вас зарегистрируют. Проблема возникает тогда, когда вор, пытающийся выдать себя за вас, делает тот же выбор. Вместо того чтобы подбирать пароль, все, что он должен сделать, — это угадать ваш любимый цвет (может быть, голубой?) и вычислить кличку вашего пса (а не посылали ли вы подписанное фото вашего Ровера на школьный сайт, участвуя в каком-нибудь конкурсе или проекте?).

Если вам предложат подсказку такого рода при создании важной для вас учетной записи, выберите вопросы, ответы на которые атакующий не сможет узнать, исследуя ваши привычки и вкусы. И нет никаких правил относительно того, как правильно отвечать на секретные вопросы. Вы можете, например, назвать кличку собаки своего приятеля, или свой самый нелюбимый цвет, или вы можете сказать, что ваш любимый цвет — Ровер, а кличка собаки — Пурпурный. Вам нужно только помнить свои неправдивые ответы на эти вопросы.

Это очень хорошие советы для всех — за исключением обычных людей. Большинство из нас используют слишком много паролей и не в состоянии запомнить их все. Более практичен такой подход: использовать один и тот же пароль для учетных записей, которые нестрашно утратить, например предназначенных для чтения онлайновых газет.

Используйте отдельный, длинный и трудноугадываемый пароль для важных для вас учетных записей (например, применяемых при перечислении через Интернет денежных сумм).

Если вы боитесь, что забудете пароль, запишите его, но в безопасном месте, а не на стикере, приклеенном к монитору.

Отнеситесь серьезно к нашему предупреждению о нежелательности использования пароля, который можно найти в словаре! Хакеры пытаются найти дыры в защите вашего брандмауэра каждый день, и было бы глупо использовать пароль в виде какого-то английского слова (допустим, слова *weather* "погода"). Хакерам понадобится меньше двух часов для проникновения в ваш компьютер с помощью подбора английского слова, если вы имели неосторожность использовать его в качестве пароля.


При конструировании пароля используйте в словах числа и знаки пунктуации, или соединяйте два слова с использованием какого-то числа, или переставляйте буквы слова в обратном порядке. Используйте как прописные, так и строчные буквы. Если вашего ребенка зовут Ваня или Маша, а номер вашего дома 426, как насчет пароля `Ivan426mashA`? Неплох также метод использования первой буквы каждого слова в какой-то фразе. Если ваша любимая песня начинается со слов "Не смотри, не смотри ты по сторонам...", нетрудно будет запомнить пароль типа `Nsnstps2006`. Неплохая идея, не правда ли?

## Позаботьтесь о безопасности — своей собственной и близких

Вирусы, шпионские программы, фишинг, всплывающие окна, спам... Стоит ли "Всемирная паутина" того, чтобы подвергаться всем эти опасностям? Нет, вы не должны приходить в отчаяние или плохо относиться к Интернету. Просто нужно принять некоторые дополнительные усилия, обеспечивающие безопасность. В дополнение к технологическим способам решения этих проблем, о которых мы уже говорили (антивирусные программы, сканеры шпионских программ, блокираторы всплывающих окон), вы должны применять маленькие хитрости ради обеспечения безопасности. Вот их краткий перечень.

- ✓ **Придерживайтесь разумного скептицизма.** Если какие-то предложения слишком хороши для того, чтобы быть выполненными, они, скорее всего, не соответствуют действительности. Ни у кого в Африке нет 25 миллионов долларов, которыми он готов поделиться с вами, если вы поможете вывезти их из страны. Давно известно: каждую минуту рождается простак. Но вы не должны стать одним из них.
- ✓ **Своевременно обновляйте программное обеспечение вашего компьютера.** И системы от Microsoft, и системы от Apple позволяют теперь делать это достаточно безболезненно. Пользуйтесь этим. Последние версии программного обеспечения часто блокируют дыры в системе защиты, которыми могли бы воспользоваться злоумышленники.
- ✓ **Используйте брандмауэр и регулярно проверяйте его.** Некоторые зловредные программы знают, как можно отключить защитное программное обеспечение, поэтому еженедельно проверяйте, работает ли оно. Возможно, на вашем компьютере установлен брандмауэр, встроенный в операционную систему. Убедитесь в том, что он функционирует. Мы рекомендуем задействовать маршрутизатор — устройство, которое позволит использовать одно соединение с Интернетом сразу для нескольких компьютеров (не важно, проводной он будет или беспроводной). Маршрутизатор обычно имеет

мощный встроенный брандмауэр, который намного труднее обойти или отключить зловредным программам. Такие устройства дешевы, поэтому их стоит приобрести даже в том случае, если у вас только один компьютер. Более подробно об этом говорится в главе 5.

- ✓ **Установите антивирусную и антишпионскую программы и своевременно обновляйте их.** Это может обойтись вам примерно в 25 долл. за год. Не пожалейте на это денег. В главе 4 рассказано о том, как нужно устанавливать программы такого рода на компьютер.


  Обязательно обновляйте описания файлов в вашем антивирусном программном обеспечении — по возможности автоматически и не реже, чем раз в неделю. (Именно с такой периодичностью появляются новые вирусы.) Производитель антивирусной программы должен иметь сайт, с которого можно загружать обновления; найдите его адрес в документации.

- ✓ **Не открывайте вложения в почтовые сообщения, если не знаете, от кого они получены** *или* **если не ожидаете их.** В случае сомнений свяжитесь с отправителем.
- ✓ **Не щелкайте ни на каких ссылках в электронных письмах, если не знаете, куда они ведут.** Если вы все же сделали это и обнаружили, что от вас требуется сообщить пароль, номер вашей кредитной карточки или кличку собаки, закройте окно браузера. Даже не думайте сообщать какую-то информацию о себе.
- ✓ **Выбирайте пароли, которые трудно угадать, и никому их не сообщайте.** Ни красивой женщине, которая говорит, что она — представитель компьютерной службы помощи, ни фальшивому агенту ФСБ, который разыскивает похищенного ребенка. Никому.
- ✓ **Будьте последовательны.** Если вы используете один компьютер вместе с членами своей семьи, добейтесь того, чтобы каждый из них понимал эти правила и был согласен их выполнять.

### А как насчет компьютеров Apple?

Наверняка владельцы компьютеров типа Apple Macintosh злорадствуют, читая эту главу: "У нас нет этих проблем. Почему бы вам не перейти на Маки?"

Пользователи Apple Macintosh также могут попасться на фишинг и получать "макулатурную" почту. Но сегодня почти ни один вирус, червяк или программа-шпион не действует на Macintosh. Конечно, положение может измениться, но, кажется, что приверженцы этой платформы всегда будут комфортно чувствовать себя в Интернете.

Во-первых, Маков намного меньше (по сравнению с Windows-компьютерами), поэтому вирусописателям нет смысла их атаковать — поскольку таких машин мало, вирусу негде будет распространяться. Между прочим, многие адреса в адресной книге Mac-компьютера принадлежат пользователям Windows, поэтому если Мак-вирус копирует себя, копии, которые он рассылает, не достигают цели. (Разработка вируса, который распространялся бы на обеих платформах, Mac и Windows, — задача трудновыполнимая даже в наше время.)

Во-вторых, операционная система, разработанная компанией Apple, Mac OS X, имеет меньше дыр в защите, ее труднее инфицировать.

Современные компьютеры Mac, в которых используются процессоры компании Intel, могут выполнять программы Windows или даже могут быть сконфигурированы так, что на них может выполняться собственно Windows — для запуска приложений, совместимых только с Windows.

Некоторые компании работают исключительно на компьютерах Mac. Когда им нужно выполнить что-то на ПК, они делают это в окне, открываемом на экране Mac. Круто!