Дэн Тинан

Технологические мифы — опровергнутые и подтвержденные

Не хотели бы вас разочаровывать, но Билл Гейтс не заплатит вам денег только за то, что вы перешлете ему письмо. Книги о Гарри Поттере не имеют ничего общего с секретными планами по популяризации магии и сатанизма. А история с Ричардом Гиром и его домашними животными? Мы даже не хотим ее обсуждать.

Все это, конечно, расхожие легенды, уже давно распространяющиеся по Всемирной паутине. Если вы хотите больше подобных историй — изучите материал «The Top 25 Web Hoaxes and Pranks» на сайте http://www.pcworld.com, но этот список далеко не полон. Многие образованные и опытные пользователи компьютеров верят в такие утверждения о технологиях, которые просто не соответствуют действительности.

Мы проанализировали наиболее распространенные в технологическом мире мифы и проделали кое-какую работу по выявлению реального положения вещей. Некоторые из этих мифов оказались полностью ложными, в то время как другие содержали в себе определенное зерно истины. Чтобы можно было оценить, насколько каждый из них соответствует действительности, мы ввели шкалу от 1 до 5, в которой цифра 5 означает, что утверждение полностью ложно, а 1 — что утверждение полностью истинно.

Миф 1. Большие диски следует разбивать на составные части и/или часто проводить дефрагментацию, чтобы добиться лучшей производительности

Это один из тех мифов, из-за которых при большом скоплении компьютерных фанатов в баре может начаться драка. По заявлению аналитика родственного нам сайта infoworld.com, дефрагментация большого жесткого диска улучшит производительность компьютеров под управлением ОС Windows. Насколько именно она повысится, зависит от количества файлов, изменяемых или удаляемых за день.

«Операционная система имеет глупую привычку использовать каждый свободный кластер, даже если он находится посередине занятого пространства с большим количеством данных, а в конце диска много свободного места, — говорит Марио Аписелла, аналитик Infoworld.com. — Поэтому получается, что новые файлы распределяются по всему диску, что означает увеличение числа операций позиционирования головки при считывании файла».

Но в тестах, проведенных *PC World*, не обнаружилось сколько-нибудь существенного увеличения производительности после применения набора дефрагментирующих утилит. По утверждению компании Diskkeeper Corporation, разработчика подобной утилиты, производительность возрастает, но только в том случае, если свободно как минимум 20 % жесткого диска. В двух словах: выигрыш может быть разным.

Разделение диска на два или более логических подраздела также совершенно необязательно сколько-нибудь повысит производительность вашей системы, но обеспечит целый набор других преимуществ. Например, это позволит вам предусмотреть выбор операционных систем при загрузке или отделить файлы, которые, как правило, не изменяются (вроде операционной системы и установленных приложений), от тех, которые изменяются постоянно (ваши данные и интернет-страницы). Это в свою очередь уменьшает сложности с фрагментацией файлов и делает более простым процесс создания резервных копий и/или замены операционной системы без риска потерять данные.

Миф 2. Если вы загружаете файлы из пиринговых (P2P) сетей, то организации по защите авторских прав легко смогут вас найти

Все это напоминает известный роман Джорджа Оруэлла «1984». «Если вы скачиваете фильмы, музыку или видеоигры из пиринговых сетей, файлы, которые вы загружаете, легко позволяют получить ваш IP-адрес», — утверждает представительница организации по защите авторских прав MPAA Элизабет Калтмен.

Но в BayTSP, наблюдающей за пиринговыми сетями вроде Bittorent и eDonkey, не столь категоричны. Разумеется, эта компания в состоянии зафиксировать IP-адрес получателя файлов, дату и время загрузки, а также информацию об интернет-провайдере, предоставляющем доступ, — но только в том случае, если объем загружаемого файла достаточно велик.

«Если файл довольно большой, например видеофильм или установочный файл (в отличие от одной музыкальной композиции), то очень вероятно, что BayTSP сможет идентифицировать скачивающего, прежде чем он закончит загрузку, — говорит Джим Грэхем, представитель BayTSP. — Не на 100 %, но с большой вероятностью. Мы никогда не утверждаем, что получаем полную информацию по каждому пользователю».

Установить по IP-адресу конкретное лицо или физический адрес тоже не такая простая задача. Как правило, юристы звукозаписывающих и кинокомпаний обращаются к провайдерам, представляя доказательства нарушения авторских прав. И уже дело конкретной организации, идентифицировать ли своего клиента по IP-адресу; соглашаются далеко не все.

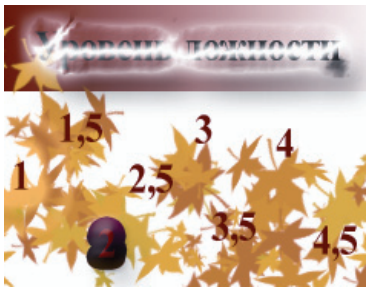
Существуют, кроме того, и другие сложности. Питер Экерсли, технолог из Electronic Frontier Foundation, говорит, что использование анонимных IP-сетей, анонимных прокси-серверов (сайты или серверы, позволяющие скрывать ваш IP-адрес) или открытых Wi-Fi-сетей может значительно усложнить задачу вашей идентификации. Но обратите внимание, что использование динамического IP-адреса, выдаваемого по DHCP, не защитит вас. Провайдеры сохраняют информацию о том, кто использовал конкретный IP-адрес в заданный момент времени, и если они захотят выдать эти данные, то вполне могут это сделать.

Миф 3. Использование высокоскоростных флэш-карт в цифровой камере позволяет снимать быстрее

Высокоскоростные карты памяти позволяют аппарату быстрее передавать изображение в файл для сохранения, но это совершенно не означает, что вы сможете сделать большее число кадров в секунду. «Когда вы делаете снимок, фотоаппарат должен получить и обработать изображение и затем сохранить его на накопителе, — говорит Майк Уонг, PR-менеджер компании SanDisk, выпускающей флэш-накопители. — Более высокоскоростная карта позволяет улучшить только вторую часть процесса — передачу файла для сохранения на карте. Если вы применяете медленные флэш-накопители в скоростных фотокамерах, то вполне можете заметить задержку во время записи файла. Но использование высокоскоростных накопителей в медленных аппаратах дает тот же эффект, что и установка резины для гоночных автомобилей на малолитражку.Разница в применении карт памяти может быть заметной в цифровых зеркальных камерах и менее ощутима в аппаратах начального уровня».

Тем не менее, добавляет Уонг, в сочетании с более производительным карт-ридером высокоскоростные карты могут уменьшить время загрузки фотографий на ПК, которое становится все более важным параметром с учетом постоянного увеличения чувствительности матриц.

Миф 4. Статические изображения на плазменных панелях «выжигают» экран, поэтому телевизор нельзя надолго оставлять включенным



Выгорание плазмы — не миф, но и не то, о чем большинству из нас стоит беспокоиться. Согласно данным сайта **http://crutchfieldadviser.com**, плазменные панели и некоторые ЭЛТ-дисплеи могут пострадать, если «неподвижное изображение, такое как видеоигра, текст с курсом валют или логотип телеканала, долго остается на экране. По прошествии времени это изображение отпечатывается на фосфорном покрытии, оставляя слабый, но заметный след на экране». Даллас Симон из **http://Crutchfieldadviser.com** говорит, что такие случаи достаточно редки, поскольку изображение все равно изменяется во время перерывов на рекламу или когда вы переключаете каналы. Но, как отмечает Андрэ Сэм, специалист по продажам из нью-йоркской компании Best Buy, с этой проблемой могут столкнуться заядлые игроки, потому что как многие игры отображают на дисплее неподвижный текст с текущей игровой статистикой — очки, полученные награды и т.п.

Однако, благодаря последним технологическим достижениям, новые плоские плазменные панели будут в меньшей степени подвержены выгоранию. «Как и любая другая вещь, если с ней плохо обращаться, она может сломаться» — отмечает Пауль Мейхофер, вице-президент по маркетингу и продуктовому планированию компании Pioneer Electronics. Но, продолжает он, для преодоления этой проблемы в новых поколениях плазменных телевизоров существенно усовершенствованы фосфорное покрытие, клеточная структура и фильтры.

Миф 5. Google находит все, что есть в Сети, и как только он заполучил вашу информацию, ее невозможно из него удалить

Хотя иногда и возникает ощущение, что невидимым пальцам Google доступно все, на самом деле это не так. Google сможет найти страницу в Сети только в том случае, если другой сайт ссылается на эту страницу, отмечает Денни Салливан, главный редактор *Search Engine Land*. «Если вы не хотите, чтобы информация была найдена, не размещайте ее в Сети или убедитесь в том, что она доступна только по паролю, — говорит он. — Google не обходит защиту паролем».

Вы также можете предотвратить индексацию вашей страницы Google или удалить из базы данных уже найденные им страницы. Для этого достаточно воспользоваться инструкциями для веб-мастеров на Google Webmaster Central. Правда, если данные о сайте уже хранятся в базе данных, пройдет какое-то время, прежде чем они будут удалены.

Гораздо сложнее удалить из Google свою персональную информацию, если она расположена на веб-сайте, который находится вне вашего контроля. Вы можете вежливо попросить владельца сайта удалить эти данные или заблокировать индексацию поисковыми системами. Если сайт содержит какую-либо личную информацию, например номер страхового свидетельства или материалы, защищенные законом об авторском праве, вы можете обратиться в Google с просьбой удалить страницу из поисковой базы. Кроме того, существуют платные сервисы вроде ReputationDefender, которые пытаются удалить из Сети недостоверную или порочащую достоинство информацию за 30 долл., но не обещают каких бы то ни было гарантий.

Миф 6. Если вы вручную вводите адрес сайта в строке браузера, то защищаете себя от хакерских атак

Самый простой способ передать свою персональную информацию в руки злоумышленников — это перейти по ссылке в сомнительном письме, пришедшем по электронной почте, и наивно заполнить все формы, запрашивающие ваши личные данные. Но и ручной ввод в строку своего браузера **http://www.yourbank.com** еще не гарантирует вас от атаки хакеров.

Остаются по крайней мере две опасности, говорит Дейв Дживанс, председатель Anti-Phishing Working Group.

Первая — это так называемый фарминг, или подмена доменных имен. В этом случае злоумышленники перехватывают запрос к сайту и перенаправляют его на какой-либо подложный сервер. Например, одна из подобных атак была направлена как минимум на 50 финансовых организаций. Дживанс говорит, что единственный способ защититься от подобных действий — это добавить в закладки браузера страницу с защищенным входом (строка адреса должна начинаться с https:), так как подобные хакерские атаки обычно нацелены на корневые страницы финансовых сайтов. Кроме того, вы в любом случае должны внимательно наблюдать за предупреждениями браузера о несоответствиях сертификата безопасности страницы, на случай если вдруг подмена адреса все же удалась.

Вторая опасность — это программы, способные вызывать такой же эффект, внося изменения в файл Hosts на вашем компьютере или каким-либо еще образом вводя в заблуждение ваш веб-браузер. Но есть немало способов обезопасить себя от подобных угроз, говорит Фред Фелман, директор по маркетингу компании MarkMonitor, среди клиентов которой — фирмы из списка Fortune 500. По словам Фелмана, если вы регулярно загружаете обновления для системы и антивирусного ПО и используете брандмауэр, то ваши шансы стать очередной жертвой существенно снижаются. А программы вроде бесплатного SpyBot Search & Destroy или WinPatrol помогут надежно защитить файл Hosts на вашем компьютере.

Миф 7. «Безлимитный» широкополосный доступ в сетях 3G действительно неограничен

Когда операторы связи продвигают свой «безлимитный» тарифный план для высокоскоростной передачи данных, очень маловероятно, что они действительно передают в ваши руки все возможности широкополосного канала. Но некоторые из операторов особенно отличились. Так, например, Verizon Vireless до недавнего времени представляла безлимитный тарифный план, который на самом деле таковым абсолютно не являлся. Хотя подписчики сервиса EVDO могли просматривать веб-страницы, а также принимать и отправлять почту, условия контракта с Verizon запрещали загрузку файлов, доступ к веб-камерам, а также использование VoIP-сервисов. Также, как потом выяснилось, компания установила «внутренний лимит» в 5 Гбайт на пользователя, при превышении которого контракт разрывался. После нескольких месяцев разбирательств Verizon добавила информацию о лимите в 5 Гбайт в лицензионное соглашение и больше не называет свой тариф «безлимитным».

В абонентском соглашении оператора Cingular (в настоящий момент — AT&T) сказано о том, что безлимитный сервис не может использоваться для загрузки аудио- и видеофайлов, а также для онлайновых игр. В отличие от Verizon в Cingular не установили определенного лимита на объем переданного трафика, хотя и могут следить за тем, чтобы эти объемы не были слишком большими.

Безлимитное предложение по использованию EVDO от Sprint не подразумевает каких-либо конкретных ограничений по виду трафика или деятельности пользователя. Однако Sprint «оставляет за собой право ограничивать или приостанавливать любое использование сервиса, связанное с постоянно высокой нагрузкой на сеть и отрицательно влияющее на ее производительность». Правда, мы пока не слышали, чтобы компания Sprint кому-то ограничила доступ, но, возможно, только пока.

Миф 8. Вы полностью защищены, когда покупаете что-либо на eBay

Крупнейший в мире интернет-аукцион и его подразделение онлайновых платежей PayPal предлагают целый набор инструментов для защиты от мошенников. Увы, эта защита в любом случае не стопроцентная.

«Когда покупатели используют PayPal для приобретения на eBay.com физически существующего товара, они автоматически получают гарантии по сделке в размере до 200 долл., — говорит представительница eBay Катерина Ингланд. — Если клиент использует PayPal, чтобы купить товар у продавца, сертифицированного как PayPal Verified, гарантии по сделке увеличиваются до 2000 долл.».

К сожалению, если вы расплачиваетесь как-либо иначе, например выписываете чек, то гарантии не действуют. Не распространяются они и на сделки с нематериальными предметами, такими как программное обеспечение или электронные документы. И если вы позволили ввести себя в заблуждение обманчивым или сбивающим с толку описанием товара — значит, вам не повезло.

Например, специалист по PR Грег П. считал, что провернет удачную сделку, когда его заявка в 300 долл. стала выигрышной в аукционе, на котором была выставлена Microsoft Xbox. Если бы Грег покупал просто сломанную Xbox, то получил бы компенсацию по сделке. Но на самом деле он приобрел текстовый документ со списком адресов, где можно купить Xbox со скидкой. Поскольку продукт был электронным, а описание лота — корректным (хотя и содержало фотографию Xbox), программа защиты покупателей от PayPal в данном случае оказалась бессильна.

Миф 9. Компьютеры от Apple неуязвимы для вирусных атак

Тем, кто безоговорочно верит в неуязвимость «Маков», пришлось недавно пройти через достаточно чувствительную проверку своих убеждений — когда специалист по безопасности Дино Дай Зови (Dino Dai Zovi) получил 10 тыс. долл. в качестве приза за взлом MacBook Pro, работающего под управлением Mac OS 10.4. Ему потребовалось менее 10 часов, чтобы найти уязвимое место в Apple QuickTime и создать веб-страницу для его использования. (Заметим, что в версии QuickTime для Windows оно также присутствует.) В последующем интервью еженедельнику *ComputerWorld* Дай Зови заявил, что операционная система Mac OS менее защищена, чем Windows Vista. (Слышите, как Стив Джобс скрежещет зубами от досады?)

Разумеется, это была не единственная брешь в защите компьютеров «Macintosh». В январе специалист по безопасности Кевин Финистер и хакер, обозначающий себя как LMH, завершили проект «Месяц уязвимых мест Apple», в котором они каждый день раскрывали новую брешь в защите «Маков». А в феврале была найдена первая уязвимая точка Mac OS 10. Хотя эксперты считают вирус OS X/Leap-A относительно безвредным, он распространяется посредством утилиты для обмена мгновенными сообщениями iChat, рассылая себя по всему списку контактов пользователя.

Однако, по большому счету, у пользователей «Macintosh» гораздо меньше вероятность пострадать от вирусов, чем у тех, кто предпочитает Windows, — хотя бы потому, что вирусов для Windows гораздо больше.

* * *

Надеемся, что это небольшое исследование поможет вам проявлять немного больше мудрости, когда вы в следующий раз столкнетесь с технологическими сплетнями, чем бы они ни были — фактами, вымыслами или чем-то средним.