ComputorEdge™ Online — 04/30/10

This issue:
Someone is Watching—Internet Scam Update

How is the Internet being used to rip off people today, and how can you protect yourself?

Table of Contents:

Windows Tips and Tricks: Shortcuts I Use the Most by Jack Dunning

Second-nature computing shortcuts for your bag of tricks.
Jack is highlighting the key combinations that he uses so commonly that he doesn't even have to think about it. Should you add any to your bag of computing tricks?

Wally Wang's Apple Farm by Wally Wang

Internet Scams
Unlike computer viruses that can be stopped and removed automatically by software, Internet scams can only be stopped through knowledge. Also, Microsoft keeps copying instead of innovating; Stellar Phoenix makes it easy for you to find and recover deleted files; a look at how statistics in marketing can lie to you; and a tip on viewing Office documents on the go with your iPad.

Linux Lessons: Do I need an antivirus program in Linux? by Pete Choppin

Recent Linux converts may wonder just how secure their Linux box is.
What's the difference between Linux and Windows machines with regards to their security approaches? With Linux, the malware game is a blessedly boring one.

Rob, The ComputorTutor: Technology Solutions by Rob Spahitz

CSS and JavaScript
Last week we looked at cascading style sheets (CSS) and a bit of how JavaScript can use the tools. This week we continue with this discussion.

Spam of the Week by ComputorEdge Staff

The latest in annoying and dangerous e-mail currently making the rounds.
This week, a reminder that anytime you see an e-mail that mentions a male-enhancement pill, it's deletion time, no matter where it appears to come from. Also, delivery companies don't know your e-mail address.

DEPARTMENTS:

EdgeWord: A Note from the Publisher by Jack Dunning

Internet scams make us more wary of salespeople and offers.
Does exposure to so much Internet bacteria through spam help to build our offline scam immune systems? If you find yourself a little more skeptical of salespeople, that may be why.

Editor's Letters: Tips and Thoughts from Readers by ComputorEdge Staff

Computer and Internet tips, plus comments on the articles and columns.

"A Look at Laser Mice," "System Spending Trends," "The iPad Is a Niche Device," "Linux Lessons: Samba," "Dell 10-Inch Netbook"

Send mail to *ceeditor@computoredge.com* with questions about editorial content.
Send mail to *cewebmaster@computoredge.com* with questions or comments about this Web site.

ComputorEdge Magazine, P.O. Box 83086, San Diego, CA 92138. (858) 573-0315

Return to Table of Contents

Digital Dave

“Digital Dave answers your tech questions.” by *Digital Dave*

Is there a free software program that lets you convert .MOV files into something manageable on a PC?; a reader wants to stop the annoying clicking sound in Internet Explorer; a reader seeks an easy way to transfer files from an old computer to a new one.

Dear Digital Dave,

I just bought a new Kodak PlaySport video camera to use for shooting my sons at bat in baseball, as well as other events. I like the camera well enough; it seems solid and takes pretty decent video. All I want to do is put some memories on disc, so down the road my kids can look back. This is my first venture into "digital" video of any kind that involves working with the video files on the computer, and at the moment it is making me long for the good old days of tape!

I spent $150 on the camera, which seemed to be a good price. However*, what the box doesn't mention is that it is starting to look like I need to spend another $100 or more to buy some decent software to work with these files. When moving my files onto my PC, I end up with .MOV files. Little did I know I would be stuck in .MOV hell!*

Give me the easy solution, Dave. When you pause/stop shooting with these cameras you cannot "pick-up" by hitting the record button again, which means every pause means a new . MOV file. Is there a way to "join" these files so you have one "movie" for viewing?

I can only seem to play .MOV files in Apple's QuickTime player (or the garbage software that came with the camera). Is there a free software program out there that lets you convert .MOV files into something manageable on a PC?

I also for some reason don't have Windows Movie Maker on my XP Pro machine, and cannot seem to find the download for it on Microsoft's site. They say to get it from the update site, but I never seem to find it there.

Help me create simple movies on my PC, Dave!

Michael Salois
El Cajon, CA

Dear Michael,

Many of the video cameras and digital cameras capable of taking video use the .MOV format. You're right that this is the Apple QuickTime format, but you are by no means stuck. There are a number of free file format-conversion programs that will make your videos usable on your

computer. One that I have used is Any Video Converter (*download.cnet.com/Any-Video-Converter/3000-2194_4-10661456.html?tag=mncol*). It is quite capable and will handle a number of common video formats. Other readers may have some recommendations of their own.

As for editing your video files (including splicing together), Windows XP does have a free download for Windows Movie Maker (*www.microsoft.com/windowsxp/downloads/updates/moviemaker2.mspx*). If someone is using Vista and is having problems with the installed version, they can download Windows Movie Maker 2.6 (*www.microsoft.com/downloads/details.aspx?FamilyID=d6ba5972-328e-4df7-8f9d-068fc0f80cfc&displaylang=en*). Windows 7, which does not come with it installed, also has a free download of Windows Movie Maker (*download.live.com/moviemaker*). Again, others with more experience with video editing might recommend other video-editing products.

Digital Dave

Dear Digital Dave,

This might be of interest for many readers: How do you stop that annoying clicking sound/noise that Internet Explorer produces continuously while browsing Web pages?

Thank you!

Max Inge
Encinitas, CA

Dear Max,

Many people are annoyed by the default clicking sound made by clicking a link in a browser or Windows Explorer. It sounds like the old drives that would chatter every time they were accessed. This is a default sound setup in the operating system.

The added clicking sound is annoying because it doesn't merely fire when you click a link, but anytime when navigation is triggered automatically. It makes it seem like it's continually clicking. Also, even if the noise were only activated for actual clicks, it's redundant because the mouse already makes a nice click sound without the computer assist. That's why it's called clicking. It's a really weird choice. If Microsoft wanted to be consistent, the computer would also make typing noises while you using the keyboard.

To change (or eliminate) the sound, open Control Panel/Hardware and Sound/Sound (Windows 7 and Vista). See Figure 1. (In XP, it's Control Panel/Sound and Audio Devices.)

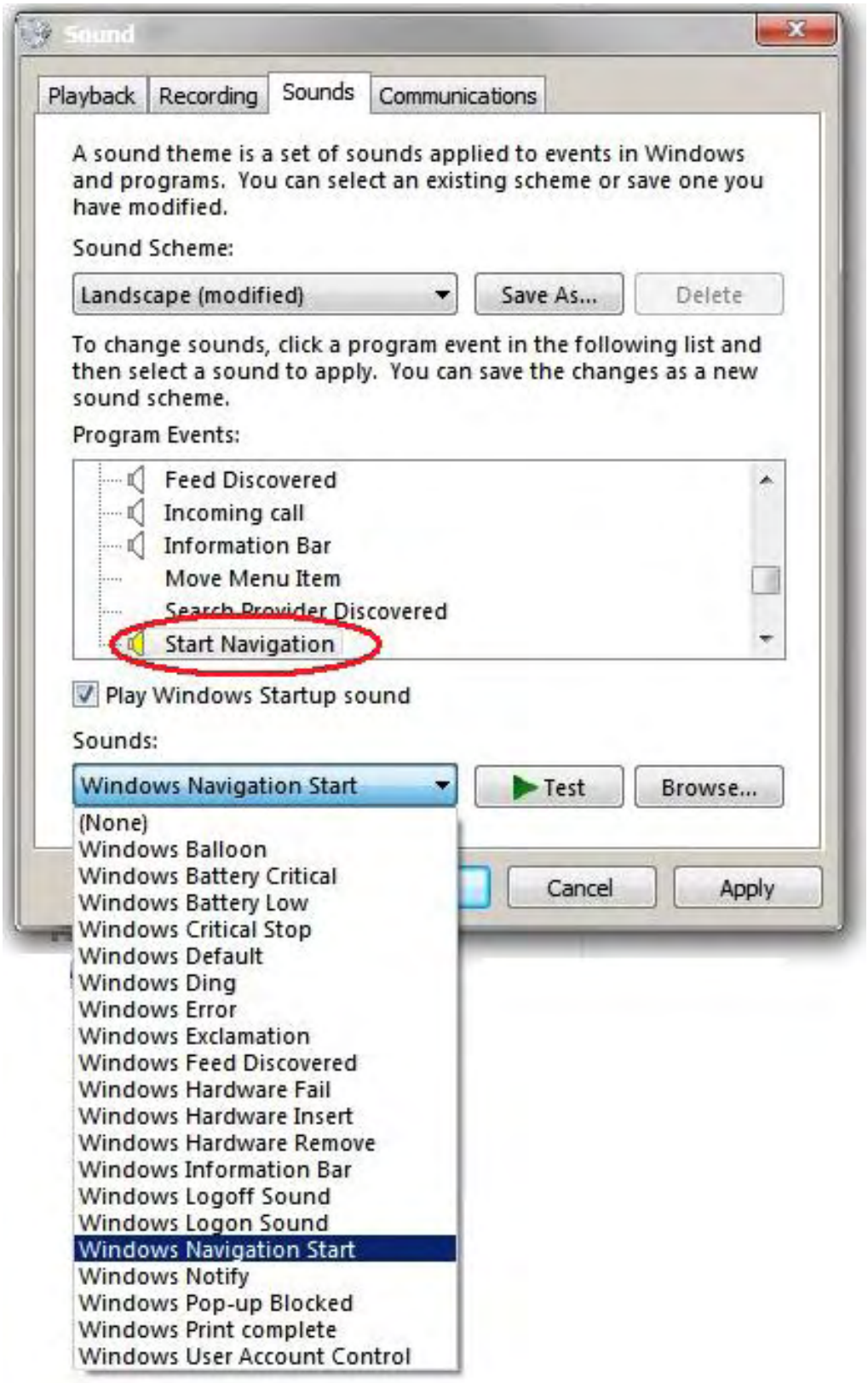


Figure 1. Sound window in Windows Vista.

Select the Sounds tab. Scroll down the list to Start Navigation under Windows Explorer. Select the sound you would like to associate with the navigation action (None is at the top of the list). Click Apply. This will change the sound when you click a link in your browser. In Windows 7 and Vista, you can test the various sounds before you pick the one that's right for you.

Digital Dave

Dear Digital Dave,

I have a Lenovo laptop running Windows 7 Pro. I just recently acquired a Compaq CQ61 notebook running Windows 7 Home premium. The keyboard on the Lenovo quit working, and I want to transfer all the programs and files from the Lenovo to the Compaq, but I can't see having the expense of buying an expensive program for one-time use only. Any suggestions?

James Murphy
El Cajon, CA

Dear James,

What you need is a USB 2.0 to SATA/IDE hard drive cable adapter. They come in many forms and cost between $10 and $20. They often have a number of parts, as shown in Figure 2.

Figure 2. A picture of a typical USB 2.0 to SATA IDE hard drive cable adapter kit.

Take the hard drive out of the Lenovo laptop and use the adapter cable to plug it into one of the USB ports in the Compaq. The drive should come up as a new external drive on the Compaq. The drive will get its power from the USB port.

The adapter can also be used to attach the internal drives from desktop computers (IDE or SATA); however, you would need to use the separate power supply and power cable provided with some of the adapter kits.

This adapter kit should be in every computer tool box. It is flexible enough to use in a variety of situations (including recovering data from many hard drive failures). Plus, if one of your friends has a similar problem, you'll look like a genius—or a nerd.

Digital Dave

Return to Table of Contents

The Dark Side of Social Media

“Harness the power of social networks without inviting in trouble.” by Michael Dillon

> With the popularity of social networking exploding over the Internet, it only stands to reason that people whose motives are sinister would also be joining the online community and looking for ways to exploit it.

Israel Hyman was very excited about his upcoming vacation from his home in Arizona to Kansas City. So excited, in fact, that he broadcast details of his trip to his 2,000 Twitter followers, including when he and his wife were leaving their house, where they were on the road, and when they arrived in K.C.

Someone, one of Mr. Hyman's followers on Twitter, took a great interest in Mr. Hyman's trip; when he returned home he found someone had broken into his house and stolen thousands of dollars in video equipment used for his business. Hyman is convinced the thieves monitored his feed to see when he would be gone, and then robbed his house. Similar incidents of thieves using Twitter to plan and execute robberies have also been reported in Florida and California.

With the popularity of social networking exploding over the Internet (Forbes estimates that 40 million people hook into Facebook, Twitter and LinkedIn each month), it only stands to reason that people whose motives are sinister would also be joining the online community and looking for ways to exploit it. Some of these exploits, such as spreading rumors about people and exposing private information, are just annoying. Others, like the aforementioned robbery of Israel Hyman and cases of financial scams via Facebook and murder threats via Twitter, are much more disturbing.

According to a recent poll conducted in the U.K., one in four people who use social media sites are revealing too much information about themselves. Sites like Facebook allow people to put in all manner of information about themselves, including but not limited to name, address (the town

in which they live), e-mail and phone number. To a trusted contact this may be harmless or even helpful information, but to criminals, they are open opportunities. According to an article in the U. K. publication *The Independent*, even trusting your friends on Facebook or Twitter with personal information may leave you open to exploitation.

"Because people control who they are friends with on Facebook, it is easy for users to have a false sense of security about the privacy of their data and activities on the site. Social engineering attacks and lax security practices by users, such as using weak passwords and design or implementation problems with the site itself, can undermine the privacy protections users rely on. Users who fall for phishing scams and get their accounts hijacked have everything in their account exposed to strangers who can then use the different types of data for identity fraud or to target the victim's friends with social engineering attacks."

As Mr. Hyman found out, posting information about your current location is now an open door for crime. Your current status, a long-favored tradition on Twitter, has often included letting your "friends" know where you are currently located. The new site Foursquare (*www.foursquare.com*) was originally conceived as a way for users to explore the cities in which they reside by meeting up with other users of the site. Users "check-in" at venues using text messaging, encouraging others in their network to meet up.

In February 2010, a Web site called "PleaseRobMe" (*www.pleaserobme.com*) pointed out that Foursquare users were inadvertently revealing "the location of empty homes." According to Wikipedia, the Dutch developers of PleaseRobMe took just four hours to build their site, which they did to point out "the dangers of sharing precise location information on the Internet."

Facebook, not unlike e-mail, has also had its users exploited by clever new fraud scams. The most common scam is for the perpetrator to hack into a Facebook account, and then send requests for money or other personal information to all the friends of the hacked account.

In February of this year, a similar attack took place in the Facebook account of a local Dallas woman. Among her friends is Dallas radio personality Mike Rhyner, who explained on his radio show that he received a message from his friend claiming she had been robbed and her cell phone was stolen. The friend's message requested $1,000, which Rhyner, thinking he was getting a message from a trusted friend, immediately wired over to an account listed in the message. "This woman is on my no-questions-asked list. If she needs something from me, I'm there; period, case closed."

Upon learning it was a scam, Rhyner immediately stopped the wire payment, and then took to the airwaves to warn his listeners. The radio station was flooded with calls and e-mails of other listeners who had also been duped by a similar scam.

Theft of personal information and scams for money are not the only types of crime currently using social media sites. On Twitter, spam posts, called "Twitomercials" have been flooding the application—businesses shamelessly pitch their products through endless repetitive streams of tweets through dummy accounts. These scams, of course, provide a link for you to click, where you may enter your contact information.

Flame wars, traditionally associated with e-mail or online user forums, have spread to Twitter, and in extreme cases have ended up with tragic consequences. In January of this year a Twitter

argument between two New York men allegedly resulted in murder; the NYPD plan to subpoena Tweets as evidence in the case, according to a newspaper report.

Jameg Blake, 22, is accused of fatally shooting Kwame Dancy, also 22, with a shotgun blast to the neck. According to the NY Daily News, Darcy and his ex-friend took a personal beef online and the taunts escalated.

So what can you do if you want to be able to harness the power of these networks without inviting in trouble? According to CNET, users of social media sites can enjoy a better sense of security by using a little common sense:

• Don't give out too many personal details about yourself, or information that might be used against you. If you don't want people calling your phone number, better not put it on your Facebook profile. Even amongst your friends, this information can be leaked out. This goes for just about anything else someone can use to take advantage of you—financial information, home address, or in the case of Mr. Hyman, the fact that you are not home.

• Use strong passwords. Most Web-based accounts, whether they are social media or e-mail, are usually hacked by the perpetrator by guessing the account password. Knowledge about you, gathered from your Facebook or any other social media page, may suggest possible passwords (such as pet names, children's names, birthdays, anniversaries, etc.). Use best practices such as including numbers, symbols, and upper and lowercase letters in passwords, making them around 12 to 14 characters and avoiding any password based on repetition or personal information.

• Don't friend/follow people you don't know or trust. It's cool to have 100,000 followers on Twitter or 1,000 friends on Facebook, but how well do you know these people? One "friend" might be monitoring your account for you to slip and reveal some useful piece of information.

• Be suspicious of communications from friends that sound unusual. When you receive a request from a friend through a social media account posting an unusual request, or worse, asking for money, be on alert. More than likely, the account has been taken over and being used to "phish" for personal information. Ask yourself: Why would my friend not call me or contact me through my personal e-mail account?

• Don't click on suspicious-sounding links or download any software (keep virus/malware protection software up to date). Malware and viruses are experiencing a boom on social media accounts. According to CNET, the biggest Facebook malware risk is Koobface (an anagram of Facebook). Once a computer is infected, it hijacks the Facebook account and sends messages to other friends of the victim, enticing them to click on a link. Twitter is also a hot ground for bad links, especially because of re-tweeting. Venture capitalist Guy Kawasaki re-tweeted a post from an unmoderated news feed and spread a Trojan to more than 139,000 followers in June 2009. Keeping your virus and malware protection software up to date will help.

• Ensure your privacy settings are set correctly. Privacy settings, especially on Facebook, change constantly. Ensure that you review and set your privacy settings on a regular basis to make sure you are controlling who has access to your information.

• Be nice. Don't get into flame wars or any other impolite behavior. Some folks just do not have a very good sense of humor, and the consequences, as Kwame Dancy found out, can be dire.

Return to Table of Contents

The Most Insidious Scams

“So-called business ventures may lure your money away.” by Pete Choppin

The latest insidious Internet scams involve entrepreneurs looking for business opportunities or turn-key ventures. If it seems too good to be true, beware.

There is an amazing amount of scams out on the Internet. Much of them prey on ordinary people just looking for an opportunity or a cause. Once such area particularly susceptible to Internet scams involves entrepreneurs looking for business opportunities, or to take on an already established so-called "turn-key" business and jut run with it.

Let's examine a few of the more insidious scams. We will describe them, then provide some clues on how to recognize and avoid them.

Some of these tips may seem a little basic. It is easy to catch yourself saying, "That could never happen to me." But don't be fooled. These con artists are clever, and even otherwise intelligent people will fall for them if they are not careful.

There is usually a common thread of deceit that runs through every one of these "programs." You need to recognize it in whatever form it takes, and the best way to do that is to become familiar with as many as possible.

The "I Want to Believe" Syndrome

Several years ago, I was invited by a trusted relative to attend a seminar where certain so-called "business opportunities" were presented. The seminar started out with dreams and aspirations. It was all about creating a vision of what your dreams were, and there was very little discussion about how this program was supposed to work, who made the money, and what exactly you did to get this money. Their main objective was to get you thinking, "I *really* want a better life for my family, and I want to believe this is going to work, so I'm going to ignore all the bad signs and keep hunting for the good news until I find it! And if I never find it...I want it anyway!!"

Even though this was not specifically an Internet scam, the same types of scams exist on the Internet. The same precautions are necessary to avoid them.

One piece of advice is, don't invest in any opportunity until you hunt down, independently, half a dozen people who have actually succeeded in the business who have absolutely nothing to gain by lying to you. Turn off your emotions as much as possible, and follow your instinct. *If it doesn't feel exactly right, don't do it!*

The Myth of MLM

The basic concept behind MLM (multilevel marketing or network marketing) is that you must build a network of contacts who will in turn build their network of contacts, and so on. The line of contacts from the lowest up to the highest is referred to as the "upline." This is the whole point to MLM businesses: to build a large upline of contacts.

The problem with multilevel marketing businesses is that they are simply not sustainable—and some may even be illegal. Eventually, those that are lower down the line become discouraged because their sales drop off.

Even with legitimate companies, your chances of succeeding big-time are slim at best. And also consider that there are a lot of people to pay. That means the prices must be inflated, which means the products are never easy to sell. And consider the fact that because it is hard to succeed, and it's generally very long before you see any real money, the vast majority of your downline will drop out or become inactive almost as fast as you can recruit them.

The myth of multilevel marketing is that anyone can make money at it, and this is simply not possible.

Work-at-Home Scams

These are the clerical, typing, filling out forms, transcription and data-entry types of services. The target of these scams is, unfortunately, the work-at-home mom who wants to earn a little money and stay home with her kids.

Many of these scams will typically claim that they have an overload of work and are looking for people who want a work-at-home opportunity to take some of their load from them.

Their logic is that they want to "follow the current trend of working with home-based individuals, just like you, to perform the data entry work," which is actually plausible because there are, in fact, legitimate businesses that do solicit work-at-home services. The difference is that a legitimate business will always look for *local* workers, not on the Internet. It's very simple: Employing people in your local area allows a legitimate business to have constant contact with their work-at-home employee.

Also consider, a real company expands nationally by increasing their customer base nationally—not by increasing their workforce nationally.

And beware of any company that wants to charge you for either the training or tools necessary to do the job. A legitimate company that hires work-at-home employees will supply the software and train you for *free*.

The Internet Mall

This is another so-called opportunity that some of my friends have tried to turn me onto. The main concept of the Internet mall is basically a Web site where you can sell merchandise that is ordered from a (hopefully) real distributor of the merchandise. The claim is two-fold. First, that the

mall has a high-traffic Internet presence, and is therefore quite lucrative. They tend to describe the Internet traffic received in a cumulative sense. For example, they might total up the hits to all the stores in their mall. Separately, each store may be getting 100 hits a month, but if it's a big enough mall, that might add up to 100,000 hits a month, and that's probably the number they're bragging about.

The second problem with Internet malls has to do with the misconception of the way they use the term "mall," and this also plays into, and is closely related, to the first claim about traffic.

There is a big difference between an Internet mall and the local mall. At the local mall, you might be heading for Sears to buy a weed whacker, and on the way you stop at the shoe store to check out their two-for-one sale, and you have to dash into the bookstore to see what new paperbacks they've got, and everyone knows it's impossible to pass the cinnamon rolls without stopping.

An Internet mall is nothing like this. The truth is it makes absolutely no difference how much traffic the mall gets. People don't go to a mall on the Internet to browse like they go to their local mall. They will go there for a specific purpose to find specific items. If someone is looking for collectible angels, they'll type "angels" into a search engine. You might believe you're in luck! The stores on both sides of you sell angels like the local mall. They can't miss you! Well, actually they can and will miss you. Search engines do not operate based on amount number of traffic a mall receives. There is just as much chance for you to get a hit as any other store on the Internet.

Be cautious when you see claims about high traffic and Internet "malls" that will draw thousands of people to your store. Where they are really making money is on the fees you pay to sign up for the mall—these can run upwards of $500 and might give you a fancy title such as "Internet Consultant." And if you start seeing training seminars for selling on the Internet, this is a definite red flag. These so-called trainings can cost you thousands.

Assemble and Sell Crafts at Home

Once, a long time ago, my wife answered an ad that claimed they were looking for talented individuals to assemble specially designed hair clips (I am sure she'll forgive me for mentioning her in this article). All you had to do was send $24.99 for a kit that you put together and send in. They would evaluate your work and then let you know if it met their standards of quality. We were told we would be notified by mail about their decision.

We sent in the money and we did, indeed, receive a kit. However, it was missing parts and the instructions were incomplete. She did her best to put together the hair clips (I think there was enough parts to assemble three clips) and she sent it in. We did get a letter that notified her that it did not meet their standards of quality. They did list the areas where she made mistakes, such as leaving glue showing, and they claimed the three clips were not uniformly made.

Here is the real flaw in these types of scams: The idea is that the company will sell the products for which *they* provide the materials, and they will reap the rewards after having paid the assemblers for their time and labor.

The money should flow in one direction only, and that is from the customer who buys the product to the company that makes the product using materials purchased by this company who will be keeping the profit, and from that company to the assembler who asks no reward other than to be *paid* for their labor.

Here are two examples of when this does *not* happen, and hence, the scam begins:

You may find the occasional "opportunity" that promises to give you the supplies free. But if you read the fine print, you'll find that's generally only after they accept a certain number of "units" (which they probably won't).

The other common scam is the occasional company that actually accepts your first shipment and sends you a paycheck. Great! Except that rarely happens more than once. See, when you take that first little paycheck to the bank, you'll be so excited you'll race right home and order more supplies, hoping to make more money—*lots* more! Then they have you and your money.

There are other problems. One is intentionally inferior material. Actually, the quality of the materials makes no difference whatsoever. Why? Because they are not *in* the business of making and selling products. They are in the business of selling unassembled material to you.

A typical tactic that they'll use as well is abuse and guilt. Often they will make you feel as though the poor workmanship is due to your inability to make a quality product, when, in fact, it is really because the product material is inferior. This is by design. They may even claim that they have several other assemblers that are able to meet their standards. All you need to do is keep working at it (and keep paying for the inferior materials).

There are many kinds of scams on the Internet and the seminar circuit. These are just a few of them. A good rule of thumb is if something feels wrong, it probably is. This is similar to the axiom, if it is too good to be true, it probably is.

Do a little research, go with your instincts and keep your emotions out of it. This will likely keep you out of most of the scams out there.

Pete Choppin has been an IT Professional for over 15 years. He currently works as a network and systems administrator for a company called Albion based in Clearfield, Utah. He has experience in all types of hardware, software, and networking technologies. He is proficient in many operating systems including Linux, Windows and Macintosh. His interests include cooking, sci-fi, computers and technology, and Web design—a semi-professional endeavor, having designed Web sites in the dental field, e-commerce businesses, and for the Boy Scouts of America.

Pete has been a devout reader of *ComputorEdge* since 1990 and contributes regularly to featured articles as well as the Linux Lessons section of *ComputorEdge*. He can be contacted at *pchoppin@comcast.net* but prefers to have comments on *ComputorEdge* articles submitted to the editor and posted for the benefit of all readers.

Return to Table of Contents

Flash Cookies and Countermeasures

“Control and delete these unwanted visitors to your hard drive.” by Michael J. Ross

> If you decide that little-understood Adobe Flash cookies are just as much a potential privacy headache as regular cookies, how do you clean them from your computer system?

Most computer users are familiar with the concept of a browser cookie, which sadly has nothing to do with raisins or chocolate chips, but instead is a piece of data that a Web site can have your browser store on your computer. For instance, when you log in to one of your favorite Web sites, and you click the checkbox to have the site remember your user name in the future (so you don't have to type it in every time you visit), then that functionality is provided using a cookie. Specifically, the site's code will request that your Web browser store your user name on your hard drive, labeled with the site's address, so it can look it up each time in the future that you visit the site.

Each cookie is a set of one or more name-value pairs. An example of this is Google storing various information in a cookie (under the site name "google.com"); within that is a name "GAUSER" associated with a value that contains your Gmail user name.

Where cookies are saved on your computer depends upon what browser you are using. For Internet Explorer, each cookie is saved in a separate text file, in a folder such as C:\Documents and Settings\Lisa\Cookies, where "Lisa" is the Windows account name for the current user. Lisa's Gmail information might be stored in a file named lisa@google[1].txt. For Mozilla Firefox, all of the regular cookies are saved in a single text file, appropriately named cookies.txt, and located in the folder C:\Documents and Settings\Lisa\Application Data\Mozilla\Firefox\Profiles\nm7rst5w.default, where the string "nm7rst5w" could be any random value (for security reasons). Other browsers naturally have their own storage and naming schemes.

Because cookies are oftentimes utilized for saving user names and other security-related data, they have been a constant source of concern to Web site owners and security experts, ever since they were first proposed and implemented at the dawn of the Web era. Privacy (or the lack thereof) has also been a major concern with cookies. They can be written to your hard drive without your knowledge. Browsers can usually store hundreds of them, and each one can contain four kilobytes of your personal information. To a certain extent, cookies can be used to track your movements on the Web, without your consent. More importantly, they can also be the target of various security attacks, such as cookie hijacking. Fortunately, all decent browsers allow you to delete cookies individually or en masse, as well as limiting which Web sites can store cookies on your computer, if any.

There is, however, a similar type of data that some argue may be an even greater security threat: so-called Adobe Flash cookies. These are chunks of data that are not stored by the browser within its conventional cookie system, but rather are stored and controlled by Flash Player. They are seen by many as especially problematic because they cannot be controlled or deleted by your browser, are subject to all of the security vulnerabilities that apply to browser cookies, can

store far more information than browser cookies, can be more difficult to find on your hard drive, and are generally less understood by the typical Internet user.

A note on terminology: Even though the phrase "Flash cookies" is widely understood and used, these Flash objects are not technically browser cookies, since they are not stored by the browser. But for most computer users, the term "Flash cookies" is far more meaningful than the unwieldy "Flash Local Shared Objects" (which could be a source of off-color jokes) or "Flash LSOs" (which sounds like something describing flying saucers).

So if you decide that these are just as much a potential privacy headache as regular cookies, how do you clean them from your computer system? We will look at three different methods, focusing on procedures for PCs running Microsoft Windows.

From the Source

Because Flash Player is the browser plug-in that creates these objects in the first place, one would hope that the company that invented Flash, Macromedia (now owned by Adobe), has provided guidance and/or a free utility for managing these objects. There is a Web page on the Adobe site that provides every visitor with their Flash Player Settings Manager (*www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html*). The Manager contains six panels: four for global settings (privacy, storage, security and notifications) and two for Web site privacy and storage. That last one, the Website Storage Settings Panel (*www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager07.html*), lists the Web addresses of all of the sites that have stored flash cookies on your computer.

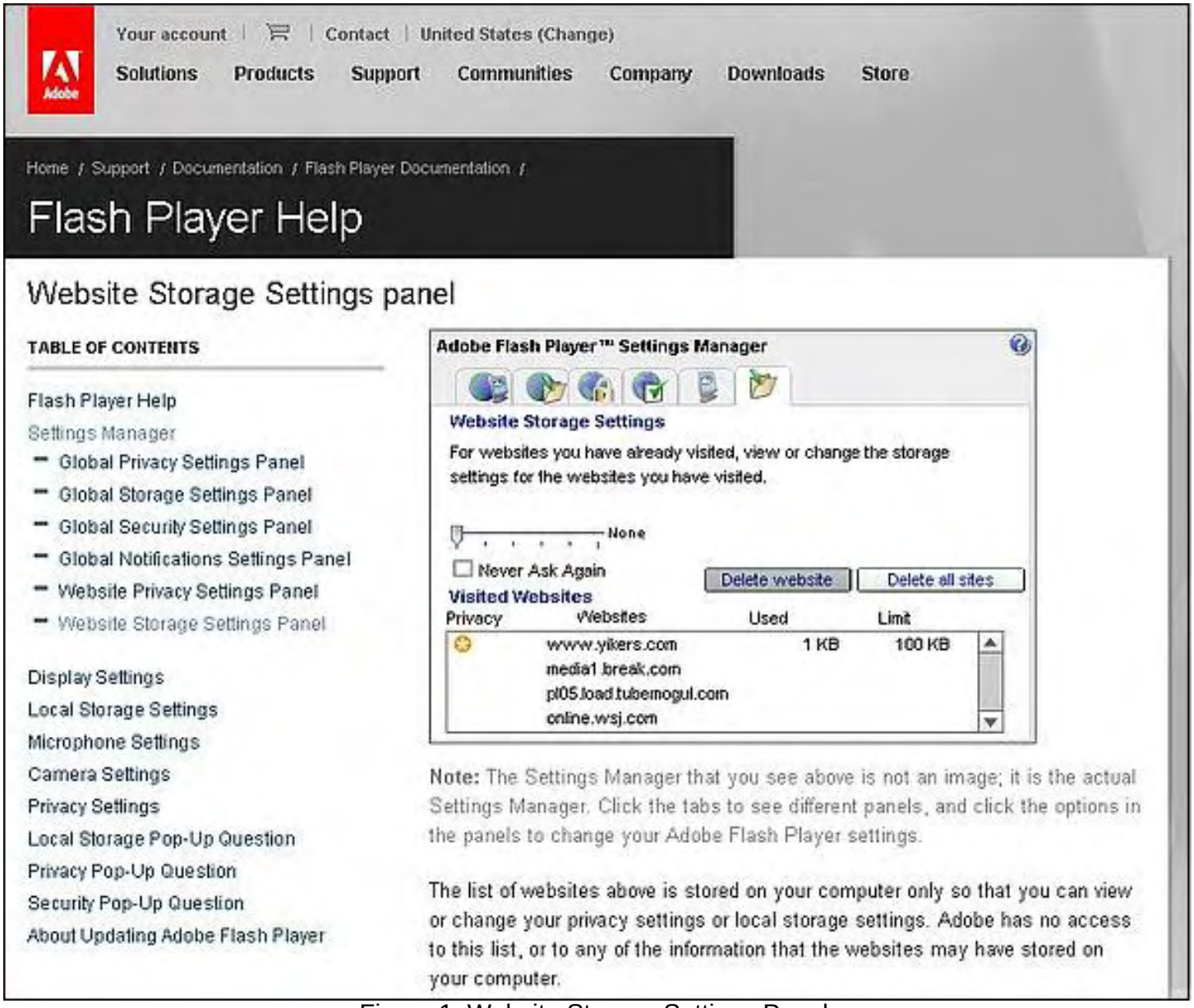


Figure 1. Website Storage Settings Panel.

For each Web site, you can see how much space has been used and the maximum allowed. You can change the latter value using the slider, from None at the far left, to Unlimited at the far right. There are also two buttons, for deleting the currently selected site, or deleting all of them—which is what you would want to choose to clean out all of the flash cookies currently on your system, to prevent those sites from accessing that data again.

To get an idea as to just how insidious these Flash cookies can be, consider the first four Web sites shown in the figure above. I have never visited any of those four, and yet all of them are listed as being visited, and have tried to store a Flash cookie on my PC. The one in the first slot, www.yikers.com, apparently succeeded in storing one kilobyte of data on my hard drive, completely unbidden. How they managed to do that is anyone's guess. Every reader is encouraged to visit that Adobe page, at the risk of being equally shocked by the number and nature of sites storing—or at least trying to store—Flash cookies on your computer.

Unfortunately, the Web site Storage Settings Panel suffers from a horrendous interface—

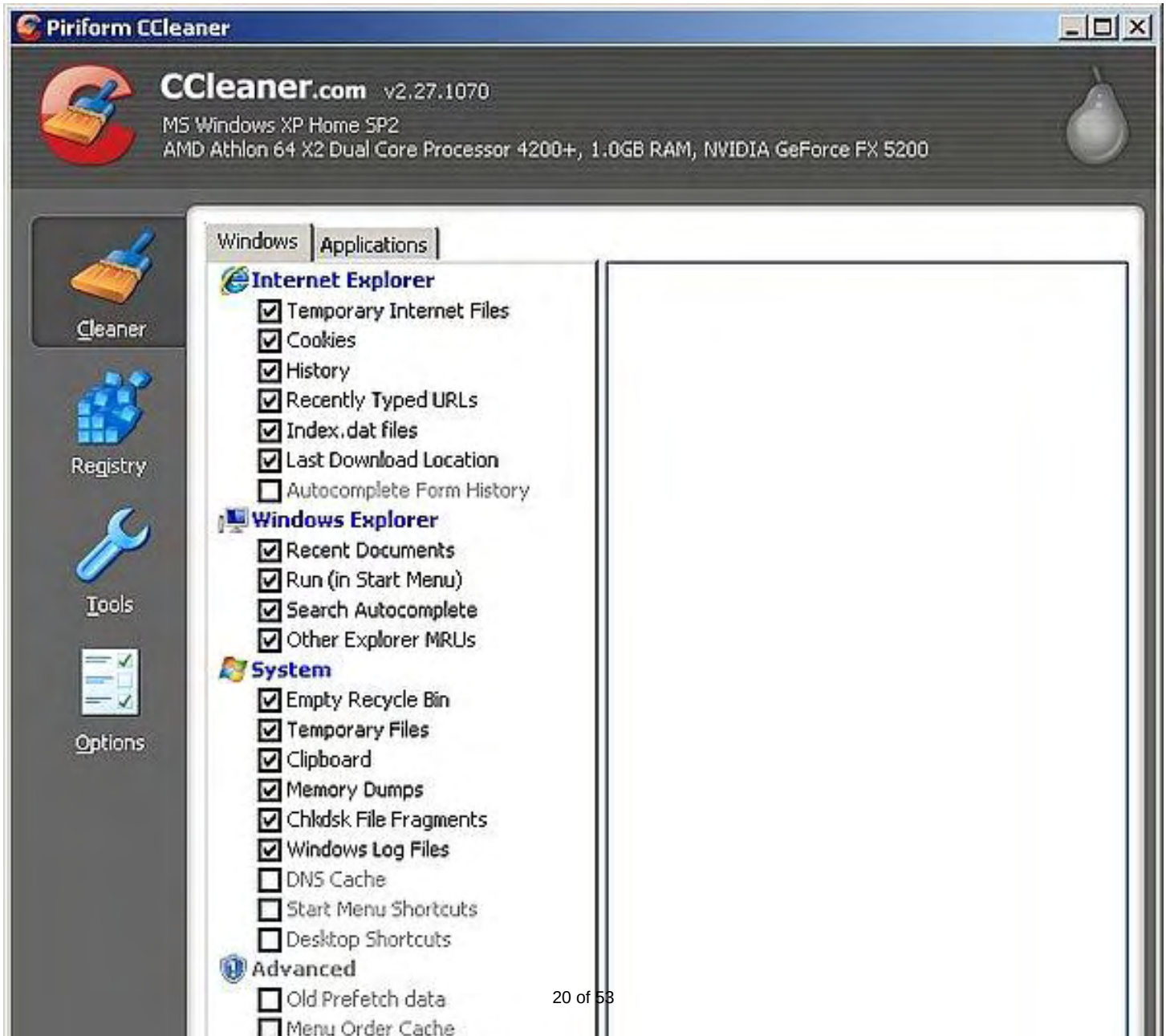
particularly the tiny list box, which displays only four Web sites at a time and cannot be re-sized. In fact, when there are hundreds of sites listed, the scroll-bar elevator icon is so small as to be unusable (assuming it even exists). You are unable to limit the sites listed using selective editing, which is a nice feature found in a growing number of dialog boxes and AJAX-powered Web pages. The Flash Player Settings Manager is perhaps best utilized as a textbook example of how not to design an interface.

"Nuke the Entire Site[s] from Orbit"

Even though Flash cookies may be far less nasty than the creatures in the movie Aliens, by the time you have discovered how many Flash cookies are on your system uninvited, and how unusable is Adobe's panel, you will probably be anxious for more drastic solutions. There are innumerable computer security and cleanup applications available that can delete Flash cookies, but perhaps the all-time favorite is CCleaner (*www.ccleaner.com/*), a utility developed by Piriform (*www.piriform.com/*). The vendor's Web site describes it well: "CCleaner is a freeware system optimization, privacy and cleaning tool. It removes unused files from your system—allowing Windows to run faster and freeing up valuable hard disk space. It also cleans traces of your online activities, such as your Internet history. Additionally it contains a fully featured registry cleaner. But the best part is that it's fast..."

Figure 2. CCleaner main page.

The site's main page has links for viewing a quick tour, and for downloading the utility. The installation process is simple and straightforward, and the default options should work fine for most users, although in the Install Options dialog box, you probably will want to disable the option—the last one on the list—to have the CCleaner Yahoo Toolbar added to your Internet Explorer, since there is no advantage to running it from your browser, and it would consume space in IE's interface. Note that the CCleaner installer vaguely refers to it as "your browser," which could be confusing to people who have (wisely) abandoned Microsoft's browser for a safer and more capable one (which includes just about all of them).



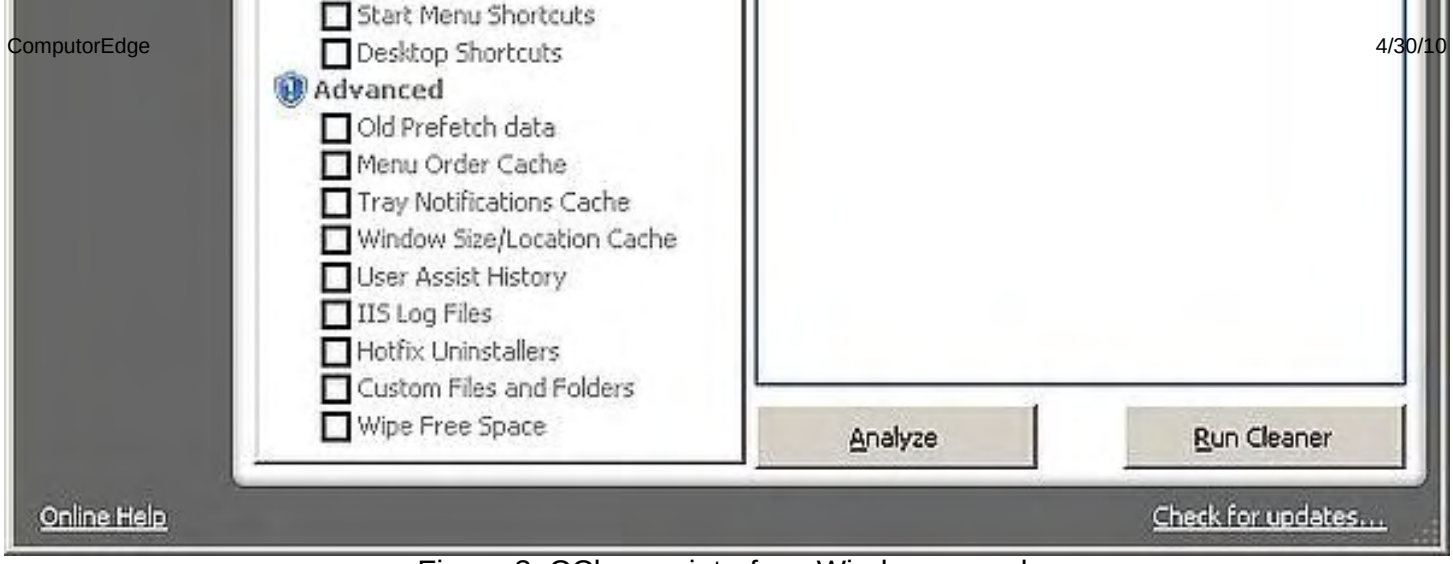
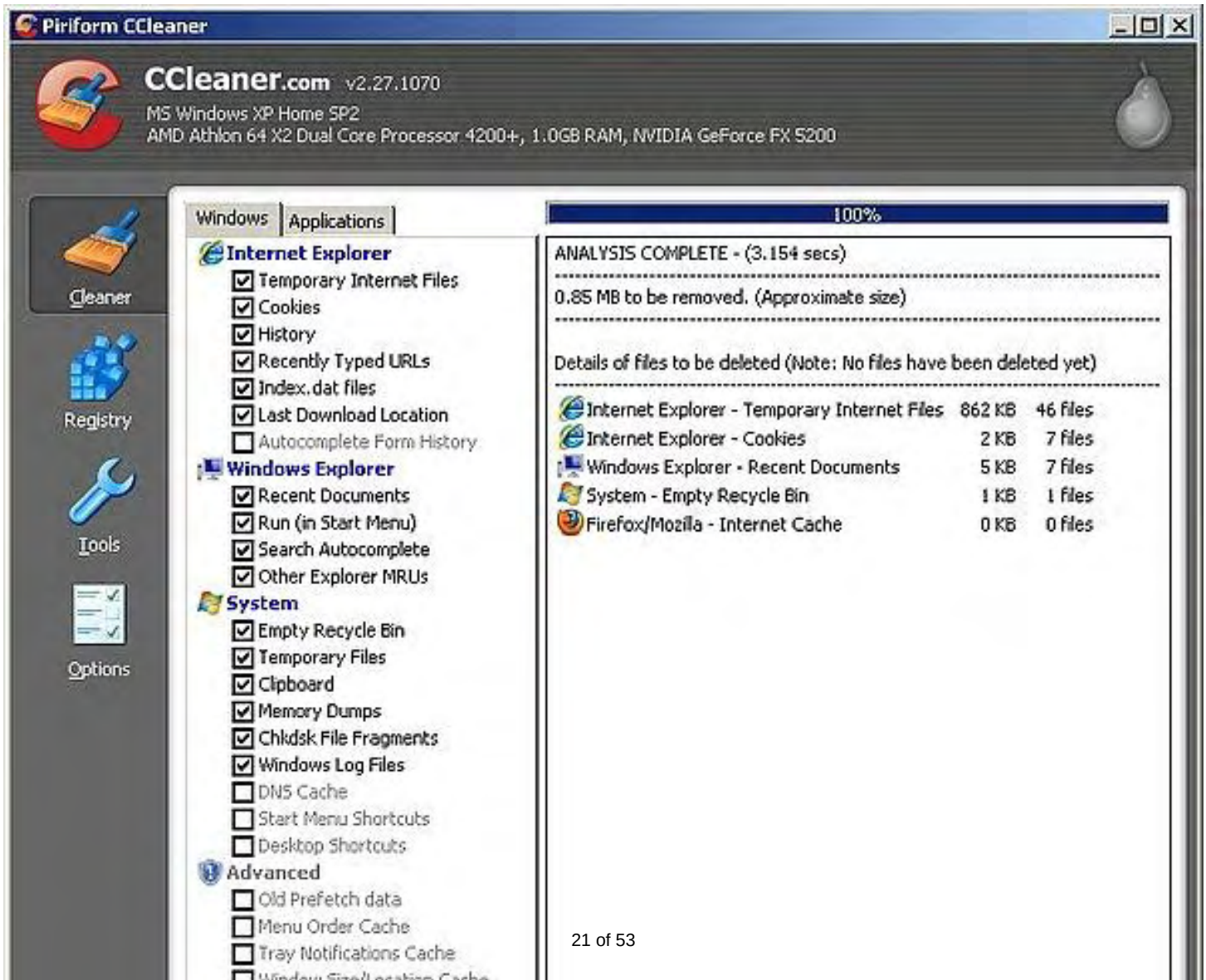


Figure 3. CCleaner interface Windows panel.

The Windows panel, which is the default, allows you to specify what types of data you want cleaned from your system—organized into four categories: Internet Explorer, Windows Explorer, operating system and advanced options. Once you have confirmed your choices, click the Analyze button to see how much data will be removed from your computer. If you need to close any applications that are currently tying up candidates files, then CCleaner will prompt you, and you won't be forced to restart the analyzing process.



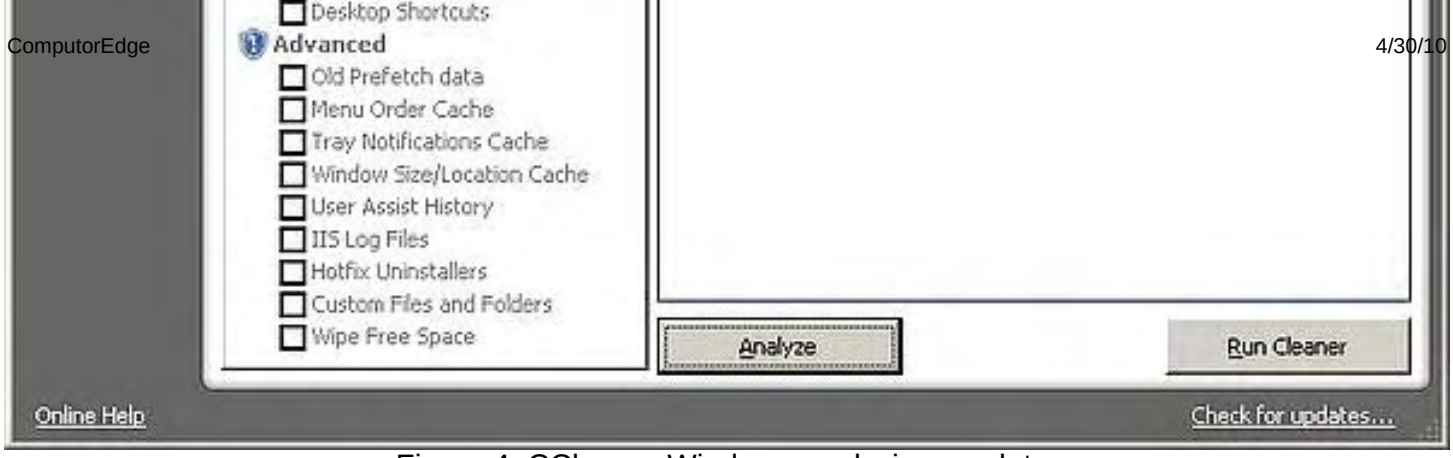
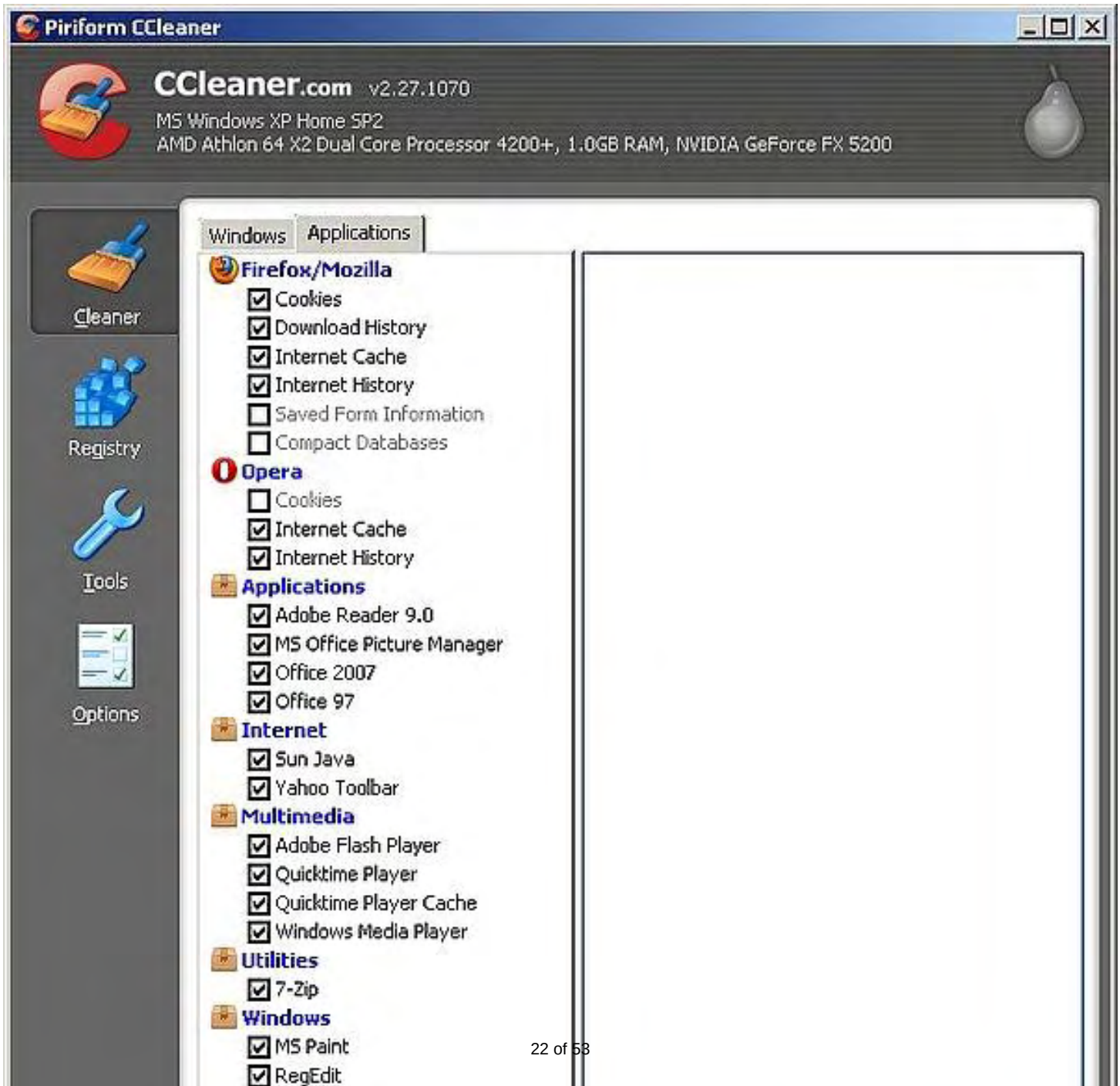


Figure 4. CCleaner Windows analysis complete.

If the analysis report does not list any data that you would not want removed, then click the Run Cleaner button. You will be asked to confirm the process, and then it will do the cleaning, usually in a matter of seconds.



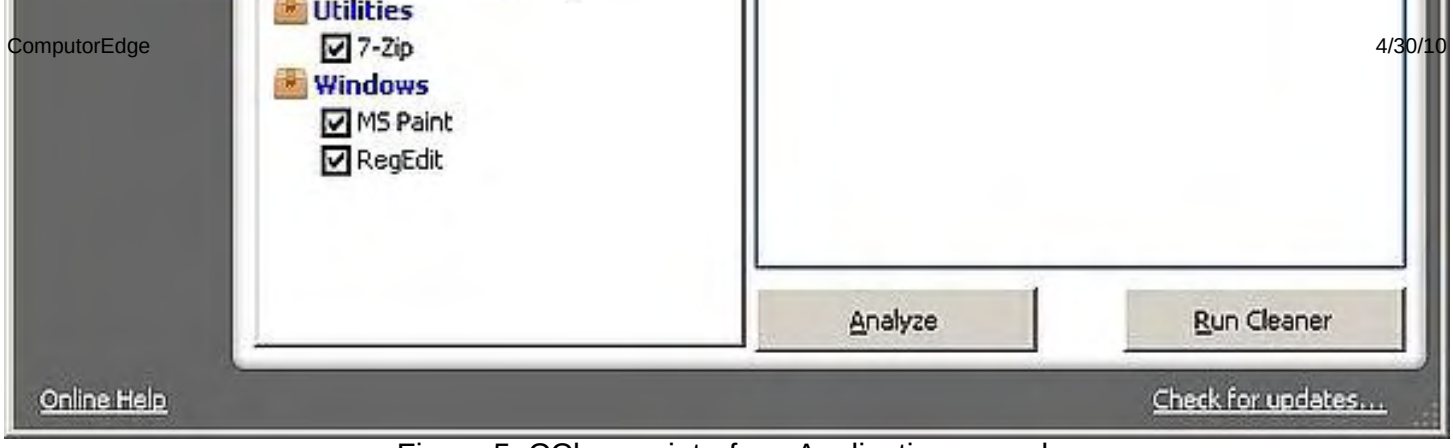


Figure 5. CCleaner interface Applications panel.

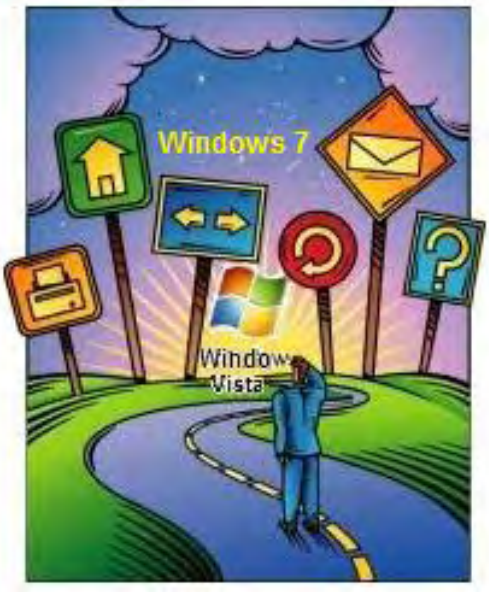
In the Applications panel, to remove any Flash cookies, make sure that in the Multimedia section, the first option is checked. Then do the analysis and cleaning procedure just as you did for the Windows panel.

CCleaner appears to be an excellent choice for cleaning the cruft out of any Windows installation. Perhaps the only obvious way that it could be improved would be for each of the 52 checkbox labels to have a tooltip (displayed on mouse hover) that summarizes what types of files the particular checkbox option will remove. Users typically much prefer this sort of immediate feedback over digging through an application's help information in hopes of finding an explanation. This is especially important for a cleanup application such as this, which involves deleting user-generated data in files whose names are not shown in the CCleaner interface.

In the final analysis, your best bet may be to skip the frustrating Adobe Flash Player Settings Manager, and go with CCleaner. "It's the only way to be sure."

Michael J. Ross is a Web developer (*www.ross.ws*), writer, and freelance editor. He creates Web sites that help entrepreneurs turn their ideas into profitable online businesses.

Return to Table of Contents



Windows Tips and Tricks

Windows Tips and Tricks: Shortcuts I Use the Most

“Second-nature computing shortcuts for your bag of tricks.” by Jack Dunning

> Jack is highlighting the key combinations that he uses so commonly that he doesn't even have to think about it. Should you add any to your bag of computing tricks?

Sometimes computer techniques are so commonly used that it's assumed that everyone knows them—and probably most people do. Yet I occasionally observe people navigating through menus when simple key combinations will do. This week I've decided to highlight those key combinations that I use so commonly that I don't even think about it. I would guess that most people know these shortcuts, but just in case I will review.

Cut, Copy and Paste

Going back to the early days of computing the Cut, Copy and Paste series has been a standard part of moving and removing text, objects and files. We've learned this series of keystrokes because they are usually listed on the Edit menu next to the associated feature.

Cut is a way to remove selected items and store them temporarily in memory to the clipboard. Since it is removed from view, it is very similar to deleting the selected object. However, a copy is maintained in the clipboard. Cut is accomplished with the CONTROL+X combination.

Copy is similar to Cut, except that the original object is not removed. It is replicated in the clipboard for later use. Copy is accomplished with the CONTROL+C combination.

Paste is the command for recovering whatever has been saved in the clipboard and inserting it at the cursor location. Paste is the completion of a move or a copy started by Cut or Copy respectively. Paste is accomplished with the CONTROL+V combination.

Most likely people use these commands so much that they don't even think about it, except when they accidentally Cut rather than Copy. The three keys (X, C and V) are conveniently next to each other, which, while easier to use, makes a slip-up much more likely (Cut rather than Copy). In those cases, an Undo is called for. Undo is accomplished with the CONTROL+Z combination. Knowing the Undo command may save a great deal of heartache.

Selecting Text and Objects

Before you can Cut, Copy or Paste, you need to select the text or object. With text it is common to hold the left-mouse button down and drag the mouse over the desired selection. (Selecting an object such as a file is usually just a click of the mouse.) However, there are a few techniques that may make selection even easier.

Double-click on a word and the entire word will be selected; triple-click for the sentence; quadruple-click for the paragraph. (This technique may vary depending upon the program that you're using.) Double-click on a file or program and the program will be launched.

If you need more accuracy in your selection, use the SHIFT key and the ARROW keys (cursors keys). While holding down the SHIFT key and moving the cursor keys, the contiguous area to the original cursor location will be selected. To speed up this selection with the mouse, after placing the cursor at the start point, move the mouse to the end point, then click the left-mouse button while holding down the SHIFT key. The entire area will be selected. This will also work for selecting groups of files (photos, music, documents, etc.) in a Windows Explorer list.

Using the SHIFT key is effective only when the selection is part of a continuous block or list. What happens when you need to select random items that are not next to each other? This is the domain of the CONTROL key. If you hold down the CONTROL key while selecting an object, other previously selected objects will not be deselected. This means that you can go through a list and select random items for cutting, copying, pasting or dragging. This is handy for situations such as picking photos to attach to an e-mail, or deleting unwanted files. Be sure to hold down the CONTROL key for each selection. Forget for just one click, and all the previously selected items will be deselected.

Another key combination I use regularly for selecting text and objects is CONTROL+A. This combination will select all the objects in a document or all the items in a list. It is very handy for copying entire sets of files.

Opening Window Explorer

Another key combination I use regularly is the Windows logo key+E. (The Windows logo key is the one with the Microsoft flag logo on it. It is between the CONTROL and ALT keys.) This opens Windows Explorer, which is the primary way to navigate your computer.

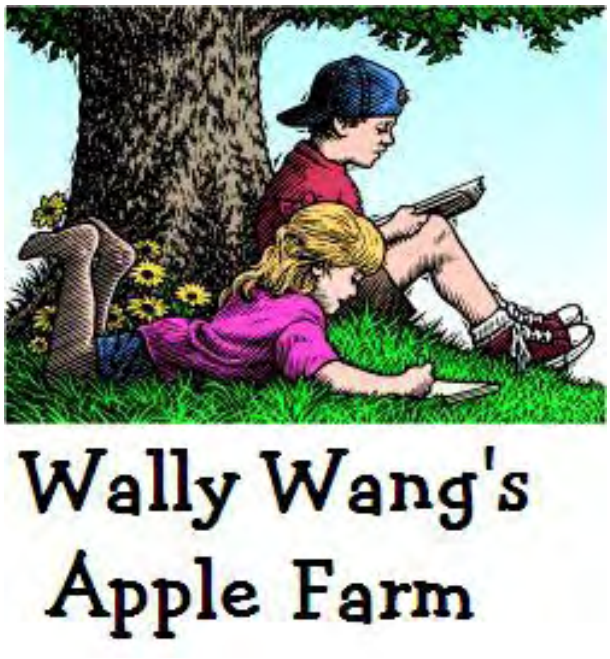
Opening Windows Task Manager

Since I learned that CONTROL+SHIFT+ESCAPE will open Windows Task Manager, I no longer use CONTROL+ALT+DELETE—which, if I make the wrong selection, is always a little dangerous. If I want to lock the screen to prevent grandkids from weighing in on my current work, I use the Windows logo key+L, which will display the logon screen.

There are other key commands and mouse techniques that I use, but those listed are by far the most common ones I employ. You may have others that you can't live without. If so, I would like to hear about them. Don't send me a list of all the other commands, just the most critical ones for you.

I have found other shortcuts that I should add to my bag of tricks, but, since they are not second nature yet, I'll save them for another column.

Return to Table of Contents



Wally Wang's Apple Farm

“Internet Scams” by Wally Wang

Unlike computer viruses that can be stopped and removed automatically by software, Internet scams can only be stopped through knowledge. Also, Microsoft keeps copying instead of innovating; Stellar Phoenix makes it easy for you to find and recover deleted files; a look at how statistics in marketing can lie to you; and a tip on viewing Office documents on the go with your iPad.

The other day I got an e-mail message claiming that UPS tried to deliver an incorrectly addressed package to my house. To claim my package, I just needed to unzip an attached file and fill in the claim form.

Then there was another e-mail message claiming that my Facebook account had been suspended and that I needed to unzip the attached file to restore my Facebook account.

Can anyone see the commonality between these two messages? Both of these messages were meant to trick me into downloading and running the attached file, which would then infect my computer.

Of course, I don't have a Facebook account, so that message was easy to ignore, but the UPS message seemed credible, especially since the e-mail appeared to come from someone with a ups.com e-mail address.

However, I ignored this UPS message for two reasons. First of all, if UPS were really trying to deliver a package to my house, how could they possibly know my e-mail address? Second, any time I get a message with a file attachment from someone I don't know, I make it a point never to download it.

Unlike computer viruses that can be stopped and removed automatically by software, Internet scams can only be stopped through knowledge. As long as you think and recognize common tricks, you can protect yourself from falling victim to nearly any Internet scam now and in the future.

The first question to ask yourself is simply, "Why me?" Most Internet scams rely on the victim's acceptance of the message's legitimacy, whether it comes from an e-mail from a relative of an oil minister in Nigeria or a sweepstakes winning notice that has randomly picked you as the million dollar winner. If you ask yourself, "Why me?" you'll often spot the absurdity of the scam's premise.

Just as it's impossible for UPS to identify someone's e-mail address from their street address, so you should always question why someone would go out of their way to contact you. If the odds that a stranger would contact you are low, chances are good that you've just identified a possible scam.

Sometimes this first test won't weed out the scams, because if you did have a Facebook account and you did receive a message claiming that your Facebook account was suspended, you might be tempted to follow the scam message's instructions. That's when you have to ask yourself a second question, "What if I do nothing?"

Most e-mail scams want you to take immediate action because the faster you follow their instructions, the faster the con artist can scam you. To urge you to take action, scams use a carrot-or-the-stick method.

The carrot is typically a large reward that if you don't take action now, you'll risk losing. The stick is the threat that if you don't take action now, you could lose something you already have, such as access to your Facebook account.

Once you identify what action a possible scam message wants you to take, do nothing. If someone were truly trying to give you vast amounts of money, they would keep trying to reach you, most likely by mail or phone. (How many strangers really know your e-mail address?)

If something truly threatening might happen if you fail to take action, you could easily verify this by contacting someone else by phone or alternate lines of communication. If you thought your Facebook account was really in danger of being shut down, just contact Facebook and ask them directly.

By not taking a scammer's expected action, you can always protect yourself from scams today and in the future. All scams tend to work alike with minor variations, whether it's an oil minister in Nigeria looking for help or an American soldier in Iraq who needs to sneak out millions with the help of another American. Once you understand how most scams work, you'll effectively immunize yourself from the effects of other scams that you might find on the Internet.

Another Head Scratcher from Microsoft

A week before April 12, Microsoft sent out invitations to a secret event, trying to mimic the excitement and secrecy that Apple announcements typically generate. On April 12, Microsoft revealed the purpose of its secret event: It was to announce a phone with a keyboard!

Figure 1. Microsoft's two new mobile phones, the Kin One and Kin Two.

If you think this announcement seems tremendously underwhelming, you're not alone. The new phones, dubbed the Kins (*kin.com*), run on a modified version of Windows CE, but can't download and install apps, are not compatible with Microsoft's older Windows Mobile 6.5, and are also not compatible with Microsoft's newer Windows Phone 7 operating system that Microsoft hopes can compete against Apple's iPhone.

The Kin's main focus is social networking, aimed primarily at the youth market. Now, maybe Microsoft will sell enough of these Kin phones to make a profit, but will the effort really be worth it? Does it make sense to release two incompatible phone operating systems? We'll find out, but if you never hear about the Kin phone ever again, you'll know the reason why.

Part of Microsoft's problem is that it's too busy trying to copy the leaders and not trying to innovate and become a leader itself. Microsoft's latest future catastrophe is Silverlight, its competitor to Adobe's Flash.

The idea behind Silverlight is to provide a better product than Adobe's Flash and become the new animation standard for the Internet. That may have sounded good a few years ago, but with Apple banning the use of Flash on the iPhone and iPad, many Web sites are dumping the use of Flash to remain compatible with the millions of iPhone and iPad users.

Instead of Flash, Apple is promoting an open standard called HTML 5. As more Web sites switch to HTML 5, reliance on plug-ins like Flash will drop. Eventually, Flash may lose all relevance altogether, much like Real Networks and its RealPlayer streaming audio/video player that nobody cares about anymore.

Of course, if nobody needs to rely on plug-ins like Flash for Web animation, they probably won't need a rival Flash plug-in like Microsoft's Silverlight either. By following a leader like Flash, and then getting blindsided by Apple's push for the open standard HTML 5, Microsoft essentially

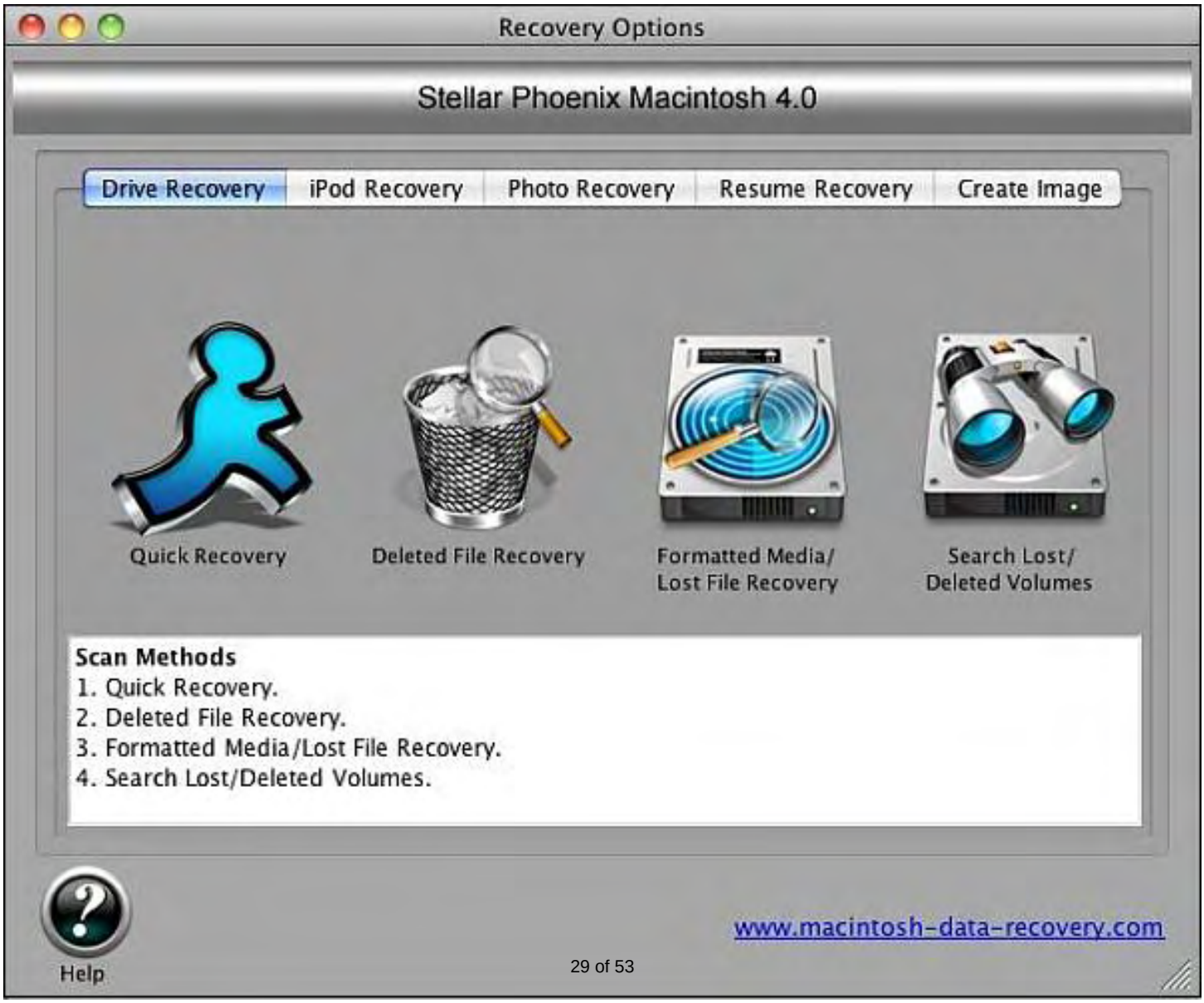
created a rival in a market that may completely disappear altogether. That will be several years of research and millions of dollars developing Silverlight down the drain, all because Microsoft chose to copy instead of innovate.

Will Microsoft ever learn? Given its past history, probably not. Maybe next month we can look forward to a Microsoft phone with a rotary dial or a Microsoft radio with vacuum tubes in a cabinet the size of a small refrigerator. Fortunately, Microsoft already offers a $12,500, 198-pound touchscreen table for those who want to buy a touchscreen computer instead of a $499, 1.5-pound iPad.

Recovering Data on a Macintosh

No matter how experienced you may be using computers, there's a good chance you'll lose an important file by deleting it by mistake or having an accident wipe it out. The safest way to protect yourself is to back up all your data automatically, such as using an external hard disk and Apple's built-in Time Machine backup program. The second safest way to protect yourself is to use a data-recovery program like the $99 Stellar Phoenix (*www.macintosh-data-recovery.com*).

Stellar Phoenix makes it easy for novices and experienced users to find and recover deleted files through a simple user interface.



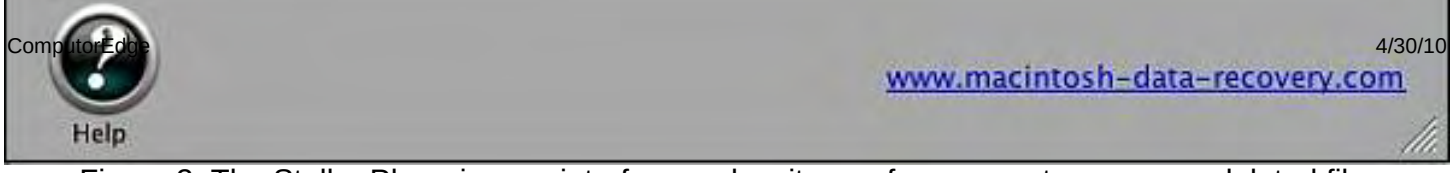


Figure 2. The Stellar Phoenix user interface makes it easy for anyone to recover a deleted file.

After a lengthy scanning process (depending on the size of your hard drive), Stellar Phoenix provides a list of file types it found. That way if you're looking for a deleted Word file (.doc), you don't waste time scrolling through a list of previously deleted MP3 or PDF files.

Figure 3. Stellar Phoenix helps you find deleted files organized by file type.

One particularly nice feature is the program's ability to recover deleted files from an iPod. If you accidentally delete a song or music video, just connect your iPod to your Macintosh and use Stellar Phoenix to retrieve the missing file. If you have a digital camera that uses a flash card like a Secure Digital or Compact Flash card, Stellar Phoenix can recover any photos you may have accidentally deleted too.

Figure 4. Stellar Phoenix can recover deleted iPod files.

Stellar Phoenix is the type of program that most people never think about until they really need it. Fortunately, you can buy and download a copy when you do need it, or just buy a copy ahead of time for added insurance. With regular backups through Time Machine, you can prevent disasters from occurring through accidentally deleted files, but for absolute protection against deleting files by mistake, you can rely on Stellar Phoenix to rescue your files and save the day.

How to Lie with Statistics

Schools emphasize reading and writing, but what they don't emphasize is how to understand the meaning behind numbers. That makes it all too easy to fool people with statistics, just as it's easy to cheat on a contract with someone who's illiterate and can't read the fine print.

To learn some of the ways to lie with statistics, grab a copy of *How to Lie with Statistics, (*www.amazon.com/How-Lie-Statistics-Darrell-Huff/dp/0393310728*)* by Darrell Huff. This book, originally printed in 1954, explains several common tricks with statistics used by advertisers, politicians and corporations to distort facts to say anything that they want.

One simple deceptive technique is to provide just enough facts to tell a lie without revealing enough facts to reveal the truth. Companies do this all the time by promoting sales of their products with claims like, "Sales increased by 50 percent over last year!"

The implication is that people are buying these products like mad, so you should consider buying one too. As author Darrell Huff explains, a 50 percent increase can still mean sales are going down and people aren't buying the product.

For example, assume that in 2008 a company sold 100 units of something. In 2009, the company experienced a 50 percent drop by only selling 50 units. In 2010, the company sold 75 units.

Comparing those 75 units to the previous year's 50 units of sales means that the 75 unit sales total represents the much-touted 50 percent increase in sales. However, by knowing the past data as well (the previous sales of 100 units), anyone could see that selling 75 units still represents a downward trend. Perhaps next year sales will continue to increase, but to claim that sales are increasing by 50 percent is technically accurate, but still misleading without all the data to examine.

Companies like Apple, Microsoft, Palm and Amazon use these tactics any time they want to imply that their products are selling like mad, so you should buy one too since they're so popular.

Another favorite tactic is to parade a list of facts, and then imply that they conclude something completely different. For example, antivirus companies love to mention the thousands of viruses capable of infecting a computer. The implication is that all of these thousands of viruses could infect and destroy your computer too, so you better buy antivirus software from us to protect your data.

What antivirus companies fail to mention is that out of the thousands of viruses available, only a handful actually have the potential to spread and infect a computer. Many older viruses only work under MS-DOS and not Windows, and can't spread unless you boot up a computer from a floppy disk. (How many computers still use floppy disks?) Therefore, the actual number of viruses that could infect a computer is far lower than the thousands that antivirus companies use to scare the public into buying their products.

Technically, they're right. Of course it sounds more impressive to say that there are thousands of viruses waiting to attack your computer rather than to state the truth and say that there are thousands of viruses, but only 10 percent of them are possible threats to your computer. Without a looming threat, it's less likely people will rush out to buy antivirus software.

Understanding the basics of statistics is crucial to avoid being fooled by advertising and marketing tricks. Even if you don't know much about statistics, a book like "How to Lie with Statistics" can help open your eyes to all the lies the computer industry (and practically everyone else) broadcasts to the public every day.

* * *

Most people use Microsoft Office on their computer, but if you have an iPad, you may want to view and edit Microsoft Office documents on the go. If you just want to view your Microsoft Office

documents on the iPad, the simplest technique is to e-mail a copy of that file to an e-mail account that you can open on your iPad. Then you can tap this attached file and view the document.

If you want to edit a file on your iPad, you'll need to download and install one or more of the $9.99 apps that make up iWork, such as Pages, Numbers, or Keynote. Then, using iTunes, you can transfer your Office files to your iPad and edit them using Pages, Numbers, or Keynote.

Just be warned that only Pages can export your document back into a Microsoft Office file. If you import an Excel spreadsheet into Numbers or a PowerPoint presentation into Keynote, you can only export those files back out again as PDF files.

In the early days, before Wally became an Internationally renowned comedian, computer book writer, and generally cool guy, Wally Wang used to hang around The Byte Buyer dangling participles with Jack Dunning and go to the gym to pump iron with Dan Gookin.

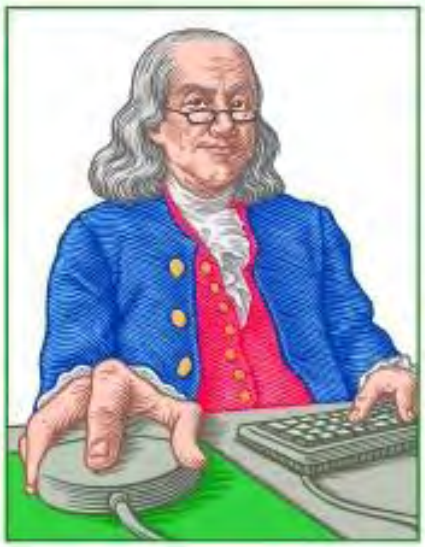
Wally is responsible for the following books:

• Microsoft Office 2007 for Dummies (*www.amazon.com/gp/product/0470009233?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=0470009233*),
• Beginning Programming for Dummies (*www.amazon.com/gp/product/0470088702?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=0470088702*),
• Breaking Into Acting for Dummies with Larry Garrison (*www.amazon.com/gp/product/0764554468?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=0764554468*), Beginning Programming All-in-One Reference for Dummies (*www.amazon.com/gp/product/0470108541?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=0470108541*),
• Steal This Computer Book 4.0 (*www.amazon.com/gp/product/1593271050?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=1593271050*),
• Visual Basic Express 2005: Now Playing (*www.amazon.com/gp/product/1593270593?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=1593270593*),
• My New Mac (*www.amazon.com/gp/product/1593271646?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=1593271646*),
• My New iPhone (*www.amazon.com/gp/product/1593271956?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=1593271956*),
• Strategic Entrepreneurism with Jon Fisher and Gerald Fisher (*www.amazon.com/gp/product/1590791894?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=1590791894*).

When not performing stand-up comedy or writing computer books, he likes to paper trade stocks with the video game Stock Reflex (*www.plimus.com/jsp/download_trial.jsp?contractId=1722712&referrer=wwang*), using the techniques he learned from a professional Wall Street day trader.

In his spare time, Wally likes blogging about movies and writing screenplays at his site "The 15 Minute Movie Method." (*www.15minutemoviemethod.com/*) Wally can be reached at *wally@computoredge.com*.

Return to Table of Contents



Linux Lessons: Do I need an antivirus program in Linux?

"Recent Linux converts may wonder just how secure their Linux box is." by Pete Choppin

What's the difference between Linux and Windows machines with regards to their security approaches? With Linux, the malware game is a blessedly boring one.

The question really is, "Do I need any antivirus software (*at all*)?" A question Windows users and recent Linux converts often ask, making a rather linear, one-for-one comparison between Windows and Linux—a classic mistake. There is much debate on this. Rather than take sides, let's examine this very crucial, if very simple, question and see if we can come up with an answer.

And the simple answer is: No, you do not need an antivirus program in Linux.

First, a Secret

There is a dirty little secret, which, if you really think about it, is kind of obvious. You don't really need an antivirus program in Windows, either. Now, the simplicity of this statement is too much to bear for most Windows users, especially people indoctrinated to believe the only thing keeping their system safe is the one little program called antivirus.

In *some* specific cases, antivirus software might be useful in helping the user decide whether the execution of a certain program might be malicious, harmful or detrimental to the health, integrity and security of his/her operating system and/or data. But the emphasis is on the word *might*.

A much better, fool-proof security is achieved by the right kind of strategy and a reasonable, layered approach to identifying threats and mitigating them. Blind fear and sheep-headed reliance on brand names is never good practice, nor will it ever make your system secure.

ComputorEdge may focus an article on Windows security and safe Web practices in the future, but this article is mainly intended for Windows users mulling a move to Linux and new, less experienced users wondering how secure their Linux box is.

Suffice it to say that a combination of keeping your Windows system updated, as well as using good Web browsing and e-mailing practices, will keep you safe. Exploiting security holes in

Windows is another matter entirely, but security vulnerabilities and virus risks are two different subjects. I will try to address some of this by comparing Linux and Windows with regards to their security approaches.

User Accounts

While Windows has always struggled with providing the world with a multiuser working environment, where there's only one admin and lots of ordinary users with limited computing powers, Linux has always done this well. Based on Unix, the operating system created from these very foundations, Linux manages to have you enjoy utmost productivity with relatively low privileges. You need not be admin to perform 99 percent of tasks.

True, in Windows you have the same mechanisms, called Limited User Account and more recently, the combination of these limitations and User Account Control (UAC), which provide a rather decent security for the user. But it can still be flaky, because most programs for Windows are created by people with the admin attitude, which makes it easier to code and deploy the software, but makes it more difficult to secure the box and prevent errors.

By running as user, by default, Linux makes both user-triggered errors and external attacks smaller in scope. While nothing can prevent deliberate self-destructiveness, the right permissions can prevent users from causing accidental damage.

This does not mean you can throw caution to the wind. Users still have full control of their own content. Nothing is easier than deleting your own files. But taking the self-inflicting metaphor further, you can still easily cut off your own arm in Linux too.

But the system remains intact. Most configurations cannot be read, let alone be changed by ordinary users. The only account in Linux that has full system access, called root, can do that. Or users that have been granted the right privileges, using the mechanism called sudo. But even then, it requires interaction and providing the right password.

Against a clueless user and automated attacks, the user account is quite sufficient. But it is not impregnable. And software does occasionally have vulnerabilities, which can be locally and remotely exploited to grant higher privileges or access to system files.

Which brings me to my second point.

System Updates

You have system updates in Windows, too, no big deal. The difference is, Windows updates are only available for *Microsoft* products. This means that programs downloaded manually will have to be periodically updated separately. Some programs make it very easy to keep them up to date, for example Firefox and Opera browsers, both of which check for patches and install them automatically, without any great hassle for the user. Others require that you uninstall the existing version, reboot, etc. All in all, almost every single Windows user is running at least a portion of his/her programs out-of-date.

This is not necessarily a bad thing. But it could be. Some programs may have vulnerabilities and they won't be solved until you proactively fix them. But when you have tens of programs waiting

for updates, this can be a serious nag. The lack of desire to maintain your machine and just run it and enjoy, the fear of things breaking up, and plain simple forgetting to update them all add up into making your system less secure than it might be.

Up until Windows 7, Microsoft updates came only once a month. Even now, they are not that frequent. This means that you were running the risk of using an operating system with potential problems for up to a month without a known resolution.

Now, let's see what happens on Linux.

Linux distributions ship as a whole—from kernel, the heart of the operating system, to every single application installed. Your distribution includes not only the critical components, it includes fonts, programs, drivers and everything else. And when you update your Linux system, you update everything.

The built-in update-management utilities with daily checks are a common thing in pretty much every single Linux distribution. You merely need to confirm the installation of available packages. You do not need to think about what needs updating, when or why. The entire thing is done automatically. It's the perfect solution for the lazy and the forgetful, as well as less knowledgeable users who won't bother with computer maintenance.

Furthermore, the distribution updates are quite frequent—every day, minimizing the window of risk when your system is exposed. Then, there's also the question of reboot. Unlike Windows, which requires frequent reboots after updates, most Linux distributions will ask for a restart only when core components are replaced, far less frequently than you're used to in Windows, making the desktop experience more streamlined and pleasant. You can actually like the system updates and not treat them as a hassle.

So the beauty of Linux system updates is you get updates for everything, including the tiniest programs, themes, fonts, icons, kernel, drivers, security patches, bug fixes, everything. All in one mouse click. Your instant messenger, your e-mail client, your browser, your office suite, your microblogging software, your Web camera drivers, your graphic drivers—every single components gets updated, automatically, all the time.

Availability of Software

Many Windows users look for programs online, going from one site to another. There are many good programs available, some of which can be downloaded from official vendor sites, others waiting for you in megasoftware index sites like Softpedia, Download.com, MajorGeeks and others. Using these is quite safe and recommended. This is the best way to ensure you get the content you want, without any undesired surprises.

Unfortunately, too many Windows users do not know where to look for software, often visiting the wrong sites, downloading the wrong software or even malicious software. Then, there's the use of cracked and pirated software, which adds yet another element of uncertainty into the equation.

In comparison, Linux users manage all their software using a centralized utility called package manager, which is tightly integrated with the update manager. The utility is a window to the software repositories provided by the distribution you're using, where you can find tons of

applications, tools, utilities and drivers for your system.

The repositories contain free and sometimes non-free (proprietary) software, including popular items like Nvidia drivers, Skype, Google Earth, Opera and many others. The content is digitally signed, so that when you download from the repositories, you know you're communicating with the real server and not a rogue, fake one. The use of digital signatures also makes software quality control easier and safer, reducing the chance of wrong or bad versions being either accidentally or maliciously pushed to the users.

The combination of frequent security updates for the entire system and digitally signed repositories that contain pretty much everything, both managed without even once using your browser and visiting this or that site searching for software, makes the chance of a Linux user stumbling upon a malicious piece of software rather slim.

Even in Windows, if you stick to reputable sources, download only from official Web sites and avoid pirated binaries, your chances of getting hit by a bad file are very, very low. In Linux, it's much lower, plus you have the enormous advantage of centralized software management. You simply don't need a reason to go about wandering and making mistakes.

Distribution Diversity

There are hundreds of Linux distributions around. Even though many are based on just a few big ones, cross-distribution compatibility is not that big. Sometimes you may run code built for another distribution on your own, but mostly, you will be forced to run packages specifically tailored for your own distribution.

RedHat code won't immediately run on Debian and Slackware code won't run on SUSE. Underneath, they're all the same, but different packaging and small nuances in the system conventions make the task of creating Linux malware more difficult. With hundreds of distributions and hundreds more different editions of said distributions available, writing malicious code that will target them all is near impossible. Windows is fairly easy, with just a few major versions, all rather compatible. For example, you can run DOS code on Windows 7 with a bit of sleight of hand. But try running a package meant for Ubuntu Heron on Jaunty. Just a year apart and yet you'll get into a lot of trouble.

The vast, almost infinite number of permutations containing kernel versions, patch levels, packaging, desktop environments, and software suites makes the Linux malware game a lottery.

It is possible to target specific versions, but it's a lot more work than doing the same thing in Windows. Low-hanging fruit is easier to pick. And let's face it. The virus writers simply do not want to put that much work into their efforts. It's not like they're getting *paid* to write their malicious software.

Advanced Skills

Using Linux is different than Windows. And it is not a given. While most computer users have been pretty much born with Windows in their mouth, Linux exists in a community of incredibly knowledgeable users less prone to accidentally ruining their system.

One of the main reasons for this is the fact Linux has to be installed manually, a procedure that is beyond the skill of most computer users worldwide. So is Windows installation, for that matter, but Windows comes preinstalled and prepackaged, whereas Linux is open-source software. Distributions build their own OS, including the kernel and the apps running on it. Furthermore, the very fact that someone wants to run an operating system that is not the default choice of the masses indicates a willingness to learn and explore—a huge advantage when it comes to running your machine safely and smartly.

Other Reasons

On top of these, we have a smaller Linux desktop market, which warrants smaller attention, the underdog attitude, as well as a range of various security mechanisms built into the system.

I have not really elaborated on these, as they vary from distro to distro, but there are all kinds of tools and utilities available in Linux distributions that make the system subversion more difficult. To name a few, there's SELinux, AppArmor and many others.

Conclusion

The combination of all these factors makes the Linux malware game a boring one. It's very boring on Windows, too, despite the best efforts by fear-mongers and doomsday preachers to keep the heat on. But seriously, if you don't download bad software, you won't end up with an unstable system. It's that simple.

Antivirus is just a tool, nothing more. Used properly, it can do something, but it is not necessary. However, when large companies have a keen and financial interest in selling their software, the question of security becomes one of politics. Luckily, you need not be a part of the game. You can enjoy safe, sane and pleasant computing without going overboard with worry or wasting your digital resources on inherently futile activities, like running antivirus software on your Linux box.

The only sensible application to this would be to spare your Windows friends from malware in transit, which you would be immune to, but they won't. However, this can be solved in many ways, without an antivirus tool, including not forwarding junk mail and not browsing unknown or questionable Web sites.

Pete Choppin has been an IT Professional for over 15 years. He currently works as a network and systems administrator for a company called Albion based in Clearfield, Utah. He has experience in all types of hardware, software, and networking technologies. He is proficient in many operating systems including Linux, Windows and Macintosh. His interests include cooking, sci-fi, computers and technology, and Web design—a semi-professional endeavor, having designed Web sites in the dental field, e-commerce businesses, and for the Boy Scouts of America.

Pete has been a devout reader of *ComputorEdge* since 1990 and contributes regularly to featured articles as well as the Linux Lessons section of *ComputorEdge*. He can be contacted at *pchoppin@comcast.net* but prefers to have comments on *ComputorEdge* articles submitted to the editor and posted for the benefit of all readers.

Return to Table of Contents

Rob, The ComputorTutor: Technology Solutions

"CSS and JavaScript" by Rob Spahitz

Last week we looked at cascading style sheets (CSS) and a bit of how JavaScript can use the tools. This week we continue with this discussion.

Last week we looked at cascading style sheets (CSS) and a bit of how JavaScript can use the tools. This week we continue with this discussion.

JavaScript Animations

You've probably seen applications on the Internet that require you to download a Flash player to view something on the page. Some of those "apps" are pretty amazing. However, since this uses a proprietary tool, you really don't have the ability to create those unless you pay for the tool used to build them. And, of course, you have to learn the proprietary programming language created by Adobe to let you use that tool.

Another option for creating cool apps for Web browsers is to learn the Java language and build things. There are some free Java development tools, but the learning curve for these can be rather steep since you are using tools that are not specifically designed for Web pages, but also used for desktop or other computer systems.

Of course, our job today is to use JavaScript to handle some of the basic things that can be done by these other tools. First, don't expect this to be trivial. You will have to work hard to make this collection of built-in browser features do what some of the other things do. However, understand that there are many benefits too. For one thing, the size of the files created by JavaScript versus a Flash app will likely be about 20 percent of the size. In addition, nobody will have to download the latest version of Flash or Java to make your stuff work; they just need a JavaScript-compatible browser, which is most of the common ones out there. One more thing, for now, is that Apple iPods do not support Flash, but they support JavaScript. That means that you can create iPod apps for people to use through their browser features.

OK now—on to animations. First a quick note about animations. There are many design considerations related to animations: What happens if two animations cross each other? Should they "collide" or simply pass by? Also, animations can consist of drawn pictures or static pictures. With drawn pictures, the time to draw then re-draw can be very slow, but you get exactly what you want when you need it. Conversely, a static picture is very quick to show, but will require many pictures to make them appear to animate. Also, static images are typically rectangular, so what happens when you have odd-shaped images displayed in a rectangle? The simple answer is to use a transparent background, but this is typically defined as part of the picture, not the browser, so I'll leave that up to the reader to locate in the picture editor of your choice.

On to the animation. Let's build a simple Web page with a picture. Note that the picture does not

actually have to exist for this procedure to work, since the browsers will show an image placeholder if the image is not found.

```
<html>
<body>
<img src="any_pic.jpg" />
</body>
</html>
```

Now let's update the body to add some buttons to allow the image to move left or right. Note that I have embedded this within the form tag, since that's technically where it belongs, although it can also be omitted. As part of the buttons, we'll reference two JavaScript procedures (yet to be defined) when the buttons are clicked: moveLeft and moveRight.

```
<body>
<img src="any_pic.jpg" />
<form>
<input type="button" value="Go left" onClick="moveLeft()" />
<input type="button" value="Go right" onClick="moveRight()" />
</form>
</body>
```

Now let's go create some placeholders for the JavaScript functions in the header:

```
<head>
<script language="JavaScript">
function moveLeft()
{
}
function moveRight()
{
}
</script>
</head>
```

Next, let's prepare some variables to track the location of the image. For this, we'll add a "global" variable inside the script area (var img_left), then set this in a new procedure (setUpImage) run when the body loads (onLoad="setUpImage()"):

```
<script language="JavaScript">
var img_left;
function setUpImage()
{
   img_left = 0;
```

```
}
...
<body onLoad="setUpImage()">
...
```

Now, rather than put almost duplicate code in the "left" and "right" functions, let's create a separate function, then have those two call this common routine:

```
function moveImage(Direction)
{
   img_left = img_left + Direction;
}
```

This routine (moveImage) accepts one value, which is the direction we'd like to move the image. Within the procedure, we update the global variable (img_left) that is tracking the image's location. We'll update this shortly to actually move the image.

To get JavaScript to work with moving the image, we have to set up a style for the image like we did last week. So in the header section, let's add one to place the image at 100 pixels down along the left edge of the page:

```
<style>
.ani_pic
{
   position: absolute;
   left: 0;
   top: 100;
}
</style>
```

We now assign this style to the image; while we're there, we'll also give it a name that will be needed later:

```
<img src="any_pic.jpg" name="moving_pic" class="ani_pic" />
```

Let's do a quick review of the page so far:

```
<html>
<head>
<style>
.ani_pic
{
   position: absolute;
```

```
   left: 0;
   top: 100;
}
</style>
<script language="JavaScript">
var img_left;
function setUpImage()
{
   img_left = 0;
}
function moveLeft()
{
}
function moveRight()
{
}
function moveImage(Direction)
{
   img_left = img_left + Direction;
}
</script>
</head>
<body onLoad="setUpImage()">
<img src="any_pic.jpg" name="moving_pic" class="ani_pic" />
<form>
<input type="button" value="Go left" onClick="moveLeft()" />
<input type="button" value="Go right" onClick="moveRight()" />
</form>
</body>
</html>
```

Now we can see that the "left" and "right" functions need to be updated. This is simple since we've already set up the "moveImage" procedure. Let's set it up so that the image will move 10 pixels at a time:

```
function moveLeft()
{
   moveImage(-10);
}
function moveRight()
{
   moveImage(+10);
}
```

Finally, we handle the hard part: moving the image. As I looked around the Internet for different sites that handle this, I've seen different techniques. The problem is that not all of them work on

all browsers. Some seem to work only on IE browsers, and others seem to work only on Firefox/ Mozilla browsers. The following technique seems to work with both.

```
   document.images["moving_pic"].style.left = img_left + "px";
```

What this does is to look at the document's images collection and try to find the image with the specified name (moving_pic), then look at its style (as defined by its class attribute, ani_pic) and change the left portion of that style to the calculation. However, the style's left property is not a number. Rather it is a number followed by the measurement type, which, in this case, is pixels. So to make this work, we set the style's left to something like 20px or -15px. This is now handled by the buttons.

When we add this to the Move function, the buttons should now work:

```
function moveImage(Direction)
{
   img_left = img_left + Direction;
document.images["moving_pic"].style.left = img_left + "px";
}
```

Now, just for fun, update the body tag so that the image moves when you move the mouse:

```
<body onLoad="setUpImage()" onMouseMove="moveRight()">
```

And to make this more interesting, you could have the image bounce back and forth along the browser as the mouse moves. For this, we'll need to keep track of the direction we'd like the image to go, so that it will give the bouncing effect. Let's change the above to point to a new procedure that will handle this for us, and then call it a wrap on JavaScript:

```
<body onLoad="setUpImage()" onMouseMove="moveBounce()">
var nextDirection = +10;
function moveBounce()
{
   docWidth = document.body.offsetWidth;
   if(img_left < 0)
   {
      nextDirection = -nextDirection;
   }
   else if(img_left > docWidth)
   {
      nextDirection = -nextDirection;
   }
   moveImage(nextDirection);
}
```

Here I capture the document width into a variable. There may be issues with some browsers for this line, but it seemed to work on the browsers I tried (IE 6.0, FireFox 3.6, Chrome 4.0). Let me know if you have a browser that doesn't work.

Moving on, I check to see if the current left position of the image is off the left edge or right edge, at which point, I change directions. I could have combined these into a single test, but decided it was cleaner to separate them.

Also, technically, when checking to see if the image is greater than the document width, you should check the right edge of the image, which is the img_left plus the width of the image. I leave that to the reader to experiment to get this right.

So wrapping up our JavaScript image animation, we end up with the following page:

```
<html>
<head>
<style>
.ani_pic
{
   position: absolute;
   left: 0;
   top: 100;
}
</style>
<script language="JavaScript">
var img_left;
function setUpImage()
{
   img_left = 0;
}
function moveLeft()
{
   moveImage(-10);
}
function moveRight()
{
   moveImage(+10);
}
function moveImage(Direction)
{
   img_left = img_left + Direction;
   document.images["moving_pic"].style.left = img_left + "px";
}
var nextDirection = +10;
function moveBounce()
{
   docWidth = document.body.offsetWidth;
```

```
   if(img_left < 0)
   {
      nextDirection = -nextDirection;
   }
   else if(img_left > docWidth - document.images["moving_pic"].width)
   {
      nextDirection = -nextDirection;
   }
   moveImage(nextDirection);
}
</script>
</head>
<body onLoad="setUpImage()" onMouseMove="moveBounce()">
<img src="any_pic.jpg" name="moving_pic" class="ani_pic" />
<form>
<input type="button" value="Go left" onClick="moveLeft()" />
<input type="button" value="Go right" onClick="moveRight()" />
</form>
</body>
</html>
```

Feel free to have fun with adding a feature to let the image move up and down and bounce off all sides.

Next week, we move on to something new: word processors.

Rob has been in the computer industry for over 25 years and is currently a part-time teacher, offering classes in Excel, Access, Visual Basic, and a variety of other technical tools. He has loved *ComputorEdge* since 1990 and can be contacted at *RSpahitz@Dogopoly.com*.

Return to Table of Contents

Spam of the Week

“The latest in annoying and dangerous e-mail currently making the rounds.” by ComputorEdge Staff

This week, a reminder that anytime you see an e-mail that mentions a male-enhancement pill, it's deletion time, no matter where it appears to come from. Also, delivery companies don't know your e-mail address.

This week there are a couple of spams to note. The first appears to be from Amazon, although all of the hidden URLs have the suffix .ru (Russia)—even the one under the Amazon.com logo. Even though it purports to advertise "TomTom XL 340S 4.3-Inch Portable GPS Navigator Bundle with Case" (and other harmless products), the main graphic include a scantily clad woman offering Viagra, Levitra, Cialis, etc. (The image is not included here, since we don't want to encourage that sort of thing.) Anytime you see an e-mail with Viagra in it, it's deletion time.

Keywords are used for filtering e-mail, and because these drugs are among the most commonly found in spam, they are often blocked. (Even a mention of one of these in a title or subtitle could prevent the *ComputorEdge* subscription from getting through to many readers.) This is why graphics, which cannot be read by filters, are used.

The second spam of the week is shown in Figure 1. If you were actually expecting a delivery, then you might be tempted to open the invoice. Don't do it! UPS doesn't know your e-mail address. Even if they did, they would use another method (telephone number) rather than e-mail you.

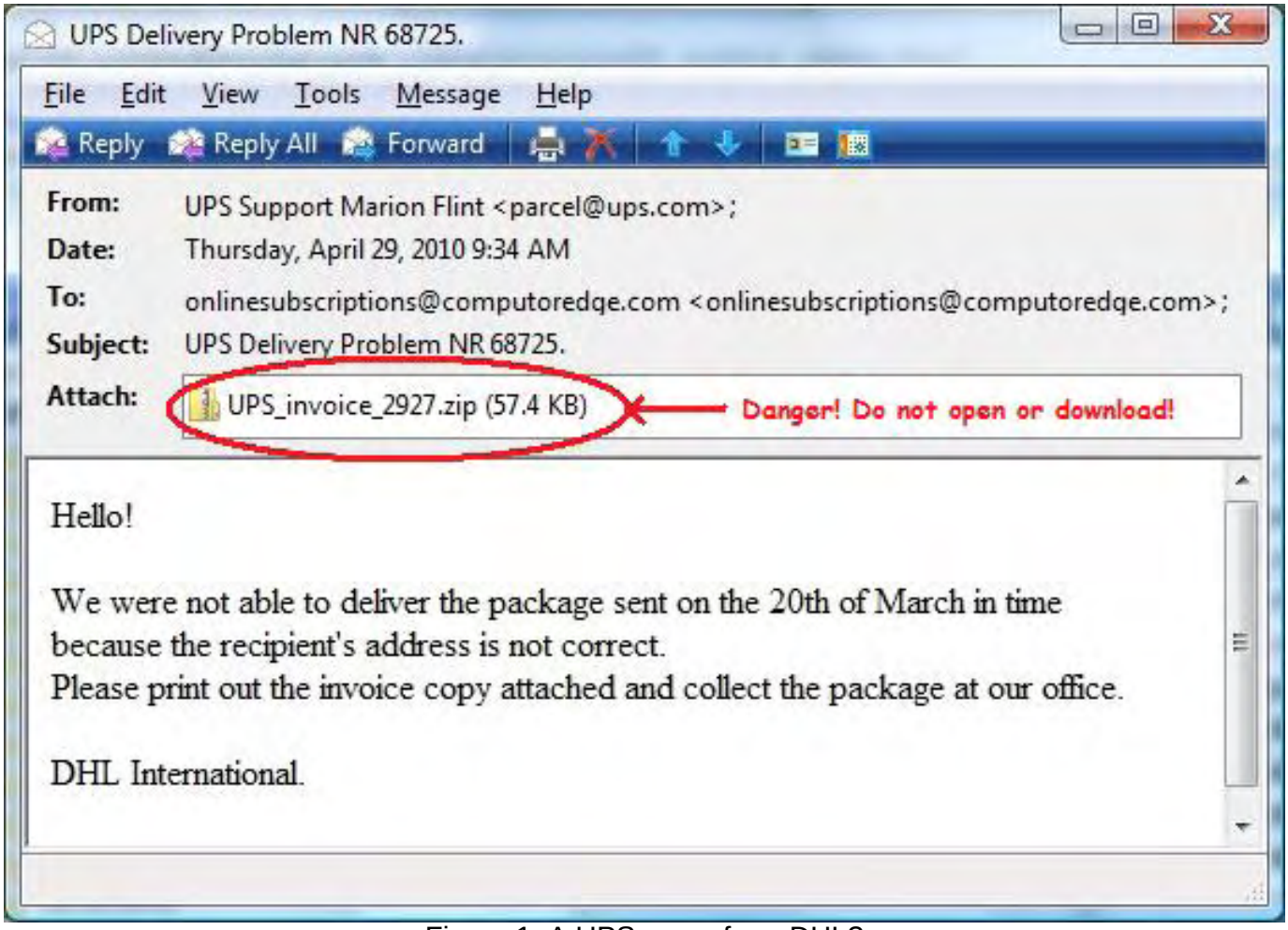


Figure 1. A UPS spam from DHL?

This is a classic phishing scheme. If you download and open the attachment, it will most likely install a Trojan horse on your computer. Whatever its purpose, it's up to no good. Another tip-off is that the spammer doesn't know that UPS and DHL are two different companies. Just delete it!

ComputorEdge always wants to hear from you, our readers. If you have specific comments about one of our articles, please click the "Tell us what you think about this article!" link at the top or bottom of the article/column. Your comments will be attached to the column and may appear at a later time in the "Editor's Letters" section.

If you want to submit a short "ComputorQuick Review", or yell at us, please e-mail us at *ceeditor@computoredge.com*.

Return to Table of Contents

EdgeWord: A Note from the Publisher

“Internet scams make us more wary of salespeople and offers.” by Jack Dunning

Does exposure to so much Internet bacteria through spam help to build our offline scam immune systems? If you find yourself a little more skeptical of salespeople, that may be why.

Maybe it's just me, but using computers and the Internet has made me more suspicious of advertising and proclamations by salespeople. Seeing regular solicitations via e-mail has made me more cautious of those that come in snail mail. It's as if the regular barrage of offers from the Internet has made me less susceptible to the usual sales pitches. Is it possible that dealing with the offers and scams that come via the Internet will actually help inoculate people against all forms of scams? I know that I don't respond well to sales pitches.

Death falls victim to identity theft.

If someone says to me, "Don't you want to make/save money?" I respond with "Not particularly." It's not that I don't want to improve my situation. It's just that I automatically identify that question as a scam—even if it isn't. (Actually, I would have no way of knowing whether a solicitation is valid or not. I never check it out because the volume spam has made me feel that virtually everyone is trying to rip me off.) If I want something, I go looking for it. Don't bother to spam me, give me a call, or send me junk mail.

One of the perverse effects of the high volume of new technology scams could be a healthy growth in the caution and suspicion of the average person. All the old scams are being attempted every day via e-mail and Web sites. With this much exposure, they become much easier to recognize—and avoid.

On the Internet, scams are not merely an occasional occurrence. In most cases, spam is arriving every few minutes. After viewing a few thousands of them, even the slowest of us start seeing the patterns. We are annoyed by them (just like we are with the Virginia gnats that try to fly up our noses in the summer), but we don't pay much attention to them. If someone comes along, whether on the phone or in the mail, who fits that same pattern seen on the Internet, we are skeptical.

The breadth of the variety of scams covers almost all of those cleverly developed over centuries of conning people. With the exposure to such interesting offers, it is difficult to remain naïve when

so many different people want to meet you and/or give you money for no apparent reason. (Although I suspect that there are many people who continue to succumb because they so desperately want to believe. "You can fool some of the people some of the time, but you can fool yourself all of the time.") Or maybe the problem is deciding which of the plethora of con games to choose. In any case, we become well educated on the number and types of "opportunities" being offered to us electronically.

Actually, I have no idea if our exposure to so much Internet bacteria helps to build our scam immune systems. I probably would have been suspicious in any case. I'm that kind of a person. With all the stories we read about people running into problems with Facebook, Twitter and Craigslist, I suspect that the nefarious people who would do us harm are just becoming more creative. It seems that there is an Internet "sucker born every day."

Jack is the publisher of *ComputorEdge* Magazine. He's been with the magazine since first issue on May 16, 1983. Back then, it was called *The Byte Buyer*. His Web site is *www.computoredge.com*. He can be reached at *ceeditor@computoredge.com*

Return to Table of Contents

Editor's Letters: Tips and Thoughts from Readers

"Computer and Internet tips, plus comments on the articles and columns." by ComputorEdge Staff

"A Look at Laser Mice," "System Spending Trends," "The iPad Is a Niche Device," "Linux Lessons: Samba," "Dell 10-Inch Netbook"

A Look at Laser Mice

[Regarding the April 2 Digital Dave column:]

I don't think optical mice have laser diodes, I think they have bright red LEDs and an optical chip with a lens that can "see" the table moving underneath and provide the corresponding motion data.

-Jim, San Diego

You're right, Jim. The optical mouse does use an LED. The laser mouse uses a laser. A laser mouse is more expensive and more accurate than the LED mouse. Both have no moving parts, but you will see light coming from the bottom of the LED mouse. The laser mouse uses a frequency not in human visual range.

-Digital Dave, ComputorEdge

Optical mice have either an LED or a laser diode. The latter are usually marketed specifically as "laser mice," and promote their higher accuracy (up to 2000 DPI vs. 400-800 for LED optical mice). Unless you're a graphic artist or a gamer, the difference in accuracy is not critical.

-Fred Loucks-Schultz, Denver, CO

System Spending Trends

[Regarding the April 9 Digital Dave column:]

Well, Dave, you're absolutely right!

But the "market" for DDR2 is certainly in my case already satiated (and *fixed* size) because of 2GB software and hardware limits! I face similar limits with the $229 system w/XP I "expanded" from a puny 160GB HDD to a full 1TB drive, of which I can only use 650GB! But at $79 it certainly drives down my cost/bit and probably satiates my life to an overly full extent!

-Michael J. Viehman, Julian, CA

The iPad Is a Niche Device

[Regarding the April 9 EdgeWord: Another iPad Perspective column:]

I do think you have a point. The iPad will have a very specific niche in computing. There will be those that use it as a netbook, and this may well be a netbook killer if you think about it. A netbook is good for surfing, e-mail, document generation and some games—looks like an iPad except the iPad has an easier interface to work with. There are some definite drawbacks. The inability to multitask is one and the limitation of storage space is another. There are rumors of Apple adding multitasking (*www.montgomeryadvertiser.com/article/20100409/BUSINESS/4090321/1003/rss05*), and do not even get me started on the lack of Flash support out of the box. The fact that they are not considering Flash support right now is a strike against the device.

Just for the record, I am no fan of Apple, but I believe I will buy one of these. They are overpriced right now, so it will be a year or so before I get one. I have been looking for something relatively inexpensive to read e-books on for a long time, besides a laptop, and the Kindle just didn't do it for me. I guess if I am going to spend $300 on a device it will have to do more than read books, and that is the iPad.

The iPad has set a standard that tablet manufacturers will have a hard time matching because they are focused on full-function computing in a tablet form. You can ask any of my geek friends, I have always wanted a robust, feature-rich tablet to work on. For what I do at home and on weekends, the iPad meets in spades, and I have a desktop PC for gaming online. That desktop will be cheaper to upgrade than a laptop will ever be. Even though I understand there are some good games for iPad out there already.

I am not a fan of Apple *but* I am a fan of how Apple seems to be able to succeed in areas that others have been unable to. While it remains to be seen if the iPad will be a success, I am willing to bet it will be. Apple failures have been few and far between, and they have never been afraid to take a risk.

-TJ Hooker, St. Cloud, MN.

Linux Lessons: Samba

[Regarding the April 2 Linux Lessons: Samba column:]

I have Ubuntu Linux ver 9.10 on a laptop. I have a Windows 7 computer and a Windows XP laptop.

Is my Linux laptop considered a server for the purpose of using Samba?

-F. Montoya, Denver, Colorado

The quick answer is that anytime a computer is offering up files or programs to other computers, it is acting as a server. Therefore, yes, your Linux laptop would be acting as a server when you load Samba for use by your Windows computers. —Jack Dunning

Dell 10-Inch Netbook

[Regarding the April 2 ComputorQuick Reviews: Pretty and Pink column:]

Thanks for the succinct article describing the Dell mini 10-inch [netbook]. I had just been looking at them wondering how good they could be. The idea of something small and light is great *if* it works like an actual computer and not a cheap try.

-Janet Still, FNP-BC, Encinitas CA

ComputorEdge always wants to hear from you, our readers. If you have specific comments about one of our articles, please click the "Tell us what you think about this article!" link at the top or bottom of the article/column. Your comments will be attached to the column and may appear at a later time in the "Editor's Letters" section.

If you want to submit a short "ComputorQuick Review", or yell at us, please e-mail us at *ceeditor@computoredge.com*.
