ComputorEdge™ Online — 07/16/10

This issue:
Identification Theft

Simple, common-sense precautions can keep your private information out of the hands of would-be identity thieves.

Table of Contents:

Wally Wang's Apple Farm by Wally Wang

Security on the Internet
Simple precautions help you safely navigate the Internet without losing money to criminals. Also, people criticize Apple without first investigating the facts; InDesign now offers collaborative features; Bento is a deceptively simple yet flexible database program; and a tip on double-clicking on the title bar of a window you want to temporarily hide.

Rob, The ComputorTutor: Tech Solutions with Microsoft Word by Rob Spahitz

Word Labels
We've now finished our awesome resumes and made some terrific business cards. Now we need to mail them out, and we want the envelopes to look professional.

Worldwide News & Product Reviews by Charles Carr

The latest in tech news and hot product reviews.
Is Your Underwear As Smart As It Could Be?—Sensors will be incorporated into logic-based biocomputing systems to monitor biomarkers; iGo Green Laptop Travel Charger: One Less Vampire in the House—Uses less than 15 percent of the standby power of standard chargers; Your Vest Friend When Traveling—A look at SCOTTEVEST's gadget-lovers' garments.

DEPARTMENTS:

EdgeWord: A Note from the Publisher by Jack Dunning

Make technology work to protect yourself from ID theft.
In spite of all the new techniques for securing our information, we will always be susceptible to the actions of nefarious people. Technology is often our best defense against the technology being used against us.

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

Computer and Internet tips, plus comments on the articles and columns.
"Virtual Machines," "Outlook Express Error Message," "Cox Spam," "Keep Up the Good Work"

Return to Table of Contents

Digital Dave

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

Adding a new laptop to a wireless network appears to have booted another laptop off the connection; could antivirus software be the cause of agonizing slowdowns?; upgrading an old Windows XP computer to Win 7 can be troublesome.

Dear Digital Dave,

I gave my old laptop to my granddaughter. I had to purchase a Wi-Fi USB stick to connect her to her mom's wireless router. The laptop connects just fine. But now her mom's laptop will not connect. In fact, in the list of available wireless connections hers is not even listed, while many others are. What happened?

Steve
Escondido

Dear Steve,

Although there could be a conflict, the connection problem for Mom's laptop may not be related to adding another computer to the network. The best way to make that determination is to shut down the recently added computer to see if Mom's computer comes back onto the network. (You may need to restart Mom's computer.) If Mom's computer does not come back, then the problem is coincidental and you will need to concentrate on restoring that connection to the router. If Mom's computer does reconnect, then you may have an IP address conflict with the recently introduced laptop.

The IP address is a numerical identification that is assigned (usually by the router) to each computer as it comes onto the network (generally of the form 192.168.xxx.xxx for an internal network). Each piece of equipment on the network must have a unique address; otherwise there will be a conflict. Usually the default for a computer is automatic IP address assignment by the router, but at times there are reasons to assign a fixed IP. If turning off all equipment, including the router, then powering up the router, then each computer one at a time doesn't resolve the problem, you will need to check the properties of each network card setup for automatic versus fixed IP assignment. (Although it is normally the default, you may also need to check the router setup to ensure that it is set to automatically assign IP addresses.)

If you can't find or fix an IP address problem, then you will need to use the diagnosis/repair tools available for the computer. Don't discount the fact that the network device for Mom's computer may have gone bad—even though it would be quite a coincident. Try the daughter's USB Wi-Fi stick on Mom's laptop to determine if the wireless card on the laptop has failed. If that doesn't work, you could also try plugging Mom's laptop directly into the router via Ethernet. If that works,

then you know that the networking on the laptop still works.

The troubleshooting procedure that you will use will vary depending upon the type of computer system and operating system. A quick search of the Web should point you in the right direction. I have actually had good luck with the repair connection tool in Windows. But always remember, "Rebootion is often the solution!"

Digital Dave

Dear Digital Dave,

For the life of me, I can't figure out why, whenever I want to bring up a blank Word document from my desktop, I get a message on the bottom that reads "Running a virus scan," and slows down for that few seconds. I have Norton Anti-virus as my protector, but I don't know whether somehow it is the problem or not—or what else is going on. The same message appears when I click on my Firefox icon on the desktop for the first time. At 79 years old, patience is not among my virtues. I wonder whether I'll still be here from second to second these days.

Julianna

Dear Julianna,

What you are experiencing is not at all unusual for virus scan products, although it seems a bit excessive if the software slows things down when you're merely opening a blank document. One of the features of antivirus software is real-time checking of documents. That means whenever you open or download a file, it is scanned for safety. How much your computer will slow down depends upon the efficiency of the antivirus software and the capabilities of your computer. The delay will be more noticeable in older, slower computers.

I'm not surprised that you noticed this issue particularly when you use Microsoft's Word. Word documents from unknown sources are notorious as targets for infection. This is why any antivirus program may pay particular attention when Word is loaded.

The real-time virus checking can usually be turned off if it becomes too annoying—although this is not advisable. Perhaps switching to another security program such as the free Microsoft Security Essentials (*www.microsoft.com/security/products/mse.aspx*) would be helpful. I don't know that this would solve your slowdown problem, but it could be worth a shot.

Digital Dave

Dear Digital Dave,

I'm using MS Win XP and am ready to upgrade to Windows 7. Can I install Win 7 on top of my XP so that programs I already have, such as Quicken, TurboTax and MS Office, will still work under Win7? I want to avoid reinstalling these programs at all costs!

Mike
Cardiff, CA

Dear Mike,

Unfortunately, the answer is no. Microsoft did not create a smooth upgrade path from Windows XP to Windows 7. You will need to reinstall all of your applications one at a time. You will be able to copy all of your data files over using Windows Easy Transfer, and then restore them after you install Windows 7. Make sure you copy everything before the upgrade process. If you do the Windows 7 install without reformatting the drive, a folder named windows.old will be created with all of your old data, but I wouldn't depend upon that for backup.

Before you upgrade, ensure that your computer can handle Windows 7 by downloading and running Windows 7 Upgrade Advisor (*www.microsoft.com/windows/windows-7/get/upgrade-advisor.aspx*). If you want to ensure that your programs and other equipment with function properly with Windows 7, go to the Windows 7 Compatibility Center (*www.microsoft.com/windows/compatibility/windows-7/en-us/default.aspx*). In some cases, you may find that it is easier and cheaper to buy a new Windows 7 computer then to upgrade an older XP.

Digital Dave

Return to Table of Contents

Identity Theft Countermeasures

“Basic security precautions to protect your identity.” by Michael J. Ross

> Simple security measures may take extra time and effort, but they are nothing compared to the financial loss and sense of violation if and when you fall victim to identity theft.

After years of hearing horror stories and warnings about identity theft, a growing number of people are realizing the dangers and risks of becoming a victim, and they are fighting back. Yet at the same time, a huge number of their compatriots are still falling prey to the types of scams within this broad category—both online and off. For instance, the number of identity theft incidents in 2008, versus 2007, increased a substantial 22 percent, to 9.9 million, according to a study published by Javelin Strategy & Research on February 9, 2009.

Many cases of identity theft are unavoidable by the individual, such as when a company or government entity loses sensitive information. But far too many of the cases could have been avoided had the victim taken some basic security precautions. Before getting into the details of how to fight back, first consider the most common methods by which identity thieves gain the information that they need in order to take the place of their victims—at least, just long enough to grab some money and run.

Vectors of Attack

Similar to how central bank notes replaced gold and silver coins as money, cash was later supplanted by bank checks for larger purchases, which made it far less common for people to be walking around with sizable sums of cash on their persons. In turn, credit cards and debit cards nowadays continue to push paper checks into the dustbin of history. Thus it should come as no surprise that financial fraud at the consumer level generally targets credit and debit cards. Whereas in the past, a thief would have to physically confront and threaten his intended victim, these days such pilfering can be done over a phone line or an Internet connection. The age of

digital money has certainly given us terrific convenience, but at the same time we are far removed from our actual wealth, which now is simply represented as digits stored on computers, possibly on the other side of the country.

Modern-day highwaymen have no need to wear masks or bandannas, nor do they need to brandish firearms as they did when bringing terror to the innocent home or stagecoach. Instead, you may see only a pretty and smiling waitress, as she merely brandishes a check for lunch at your favorite restaurant, and brings to your table a chocolate mint to soften the sticker shock. But when she walks away with your credit or debit card, and moves behind the counter, it takes only a moment for her to run your card through a hidden device that reads its information, and transmits it wirelessly to an accomplice nearby, who within minutes will have e-mailed the information to others waiting to charge big-ticket items on your account, before you even leave the restaurant. In fact, some people become so adept and bold at "card skimming," that your card can remain in sight almost the entire time. In a common ruse, a larcenous waitress pretends to drop your card, and as she retrieves it from the floor, she swipes it through a skimmer hidden under a long skirt or under a serving tray.

Perhaps our modern thief is not able to obtain a job interfacing with the public—and their credit cards. That doesn't mean that your card information is impossible to obtain. Dumpster diving is not limited to homeless people looking for discarded food and clothing: Anyone can rummage through commercial trash receptacles in search of sensitive financial information, which they can use themselves for making fraudulent purchases, or sell to criminal syndicates just about anywhere on the planet with telephone and Internet service. Retailers and their customers are generally becoming more cognizant of the dangers of tossing out credit card slips, computer printouts of financial account information, etc. But the data divers keep at it, always hoping to make a quick buck from a slow learner.

Not everyone relishes the idea of leaping into dumpsters in the dark of night. A less athletic criminal may prefer "pretexting" his way into your financial life, by posing as a trustworthy person working for a legitimate company or government organization, and attempting to get you to divulge your confidential information, such as a password to a bank account, or credit card details. Let's say he is pretending to work in the online security department at a large bank with millions of customers. If the prospective mark who picks up the phone turns out to not even have an account at that bank, the criminal can simply apologize for calling the wrong phone number, and then try another number. Other possible guises include an investigator at a major credit card company, or a representative from one of the big credit bureaus. The miscreant can try to pass

himself off as a member of law enforcement, but that entails much greater risk should he get caught.

If you limit your retail purchases to cash, and you never fall prey to any pretexting attack, does that mean that you are immune to identity theft? Sadly, it doesn't, as long as you have some financial accounts online. For instance, you might receive an unexpected and official-looking e-mail message that appears to be from your online bank, Big Bux Savings. The message explains that, for whatever reason, you need to log into your account, and the nice people have helpfully included a link in the message for you to click on. You do so, and it takes you to a Web site that looks exactly like the one that you normally see when you log into your account. The only difference is that the address at the top of your Web browser is not the usual "https://www.bigbuxsavings.com/" but instead something like "http://bigbuxsavings.ix.com/" or, more brazenly, something like "http://98.76.54.32/." Your first attempt at logging in will fail—at least, from your perspective. To the criminals who created the fake Web site, your login attempt succeeded beautifully, because now they have your username and password, and will use it to drain your account as fast as they can. The favored name for this is "phishing," a term that is most likely a variation of "fishing," since the original e-mail message was acting as bait to lure the unsuspecting prey.

These are not the only ways that a tech-savvy bad guy can attempt to get your money, but they cover the majority of cases, and give you an idea of how easy it is for our reliance upon digital money to turn sour.

Vanquish Those Villainous Vectors

Even though there are innumerable identity thieves out there, continually devising new methods of attack, you can successfully defend yourself against most of them. Let's address the four major attacks listed above, in that order.

To completely reduce the risk of becoming a victim of card skimming, you could use only cash for paying for any retail goods and services. After all, credit and debit card transactions in the outside world are much riskier than those performed online. But that would be rather inconvenient in today's digital world, and would also entail the risk of carrying around a lot more cash. A better approach is to insist upon keeping your card in view throughout the entire transaction, even if that means walking over to the cashier and requesting that the check be brought over, so you can pay it right there.

The best way to combat the dumpster divers is to be vigilant about shredding any papers that you are disposing of (preferably in a recycle bin, and not the trash). Your humble paper shredder could turn out to be worth its weight in gold (or at least silver). It is admittedly more difficult to get others to follow the same best practice. In those instances where you are on the spot—such as when providing personal and financial information at a medical or dental office—be sure to ask them what happens to any printouts. If someone processes your credit card using a manual imprinter, ask for all copies that the merchant is not required to keep, so you can shred them at home. The biggest challenge is the companies that store your personal data on their computers—and even worse, share them with other companies. Any time you open an account, insist that they flag your account to not allow distribution of your data to any other company, including subsidiaries and partners. Then call back a few days later to verify that they made the change. Be prepared to be disappointed at how many companies ignore or flub the first request.

Pretexting is most efficiently defeated by simply asking for the caller's name, company and toll-free telephone number. You can tell them that you are busy at the moment, but will call back shortly. Verify the telephone number with your records, before calling. By calling the company's number yourself, and asking for the representative by name, it confirms that she at least works for the company she claimed. If the request is legitimate, then the caller shouldn't have a problem with your request, and may be impressed with your wisdom in employing this simple but effective method. But if it is a pretexting attempt, then she may hang up immediately, or give you bogus information; either way, you have nipped that attack in the bud.

Phishing is, of course, best countered by not taking the bait—in other words, never click on a link within any e-mail message if it supposedly will take you to a site where you are expected to log in. It is much safer to open a new browser window and type in the Web address of the bank or other destination, or use your bookmarks, since you probably have that address saved already in your browser. Also, if you do ever notice an address that looks suspicious, do not proceed any further, but instead follow the aforesaid procedure. In the earlier example of "http://www.bigbuxsavings.com/" versus "http://bigbuxsavings.ix.com/," the only part that matters is what is just to the left of the ".com." The "ix.com" is a red flag, while the ""bigbuxsavings" in "bigbuxsavings.ix" does not make it legitimate. Keep in mind that financial firms and other organizations that store sensitive information in accounts that you can log into should never ask you to click on a link in a message, but instead will simply instruct you to go to their site, or call their toll-free number. Lastly, your odds of inadvertently chomping on a baited hook are greatly reduced if you minimize the hooks in the water: Use an e-mail service with top-notch spam filtering, such as Gmail.

Other Strategies for Defense

Although not guaranteed to prevent you from becoming a victim, the methods outlined above can make a huge difference, especially when supplemented with additional countermeasures. When asked to give out your Social Security number by anyone other than the Social Security Administration or your employer, ask if a substitute number can be used. As noted earlier, shred all of your personal papers before tossing them in the recycle bin—particularly those from banks, credit card companies, and insurance companies. Switch to paperless account statements.

When typing in your PIN at an ATM machine, retail store, or gasoline pump, shield the keypad from prying eyes. Bear in mind that those eyes do not necessarily have to be close and looking over your shoulder; they can be in a nearby van, using binoculars. Never use an ATM machine that looks very new or in an unusual location, because fake ones have been deployed and have snared many banking customers. When going out, carry only the cards and personal information that you would need for that particular trip.

Protect your postal mailbox and its contents. Collect the mail promptly, and drop off any important outgoing mail at a post office, and not an unprotected mailbox. Stop mail delivery if you will be away for a while.

Keep an eye on your wallet or purse, even in the office. In the home, protect your confidential information from anyone outside the family, including service personnel making house calls. Avoid storing financial and other sensitive information on laptops and USB flash drives, or at least strongly encrypt it.

On your computer, be sure to use a firewall (to monitor both incoming and outgoing traffic), and periodically run up-to-date antivirus and anti-spyware programs if you ever download files or attachments from unverified sources. In fact, open attachments only from people you know and trust, and only after scanning for viruses. For surfing the Internet, use any browser instead of Internet Explorer. Never type in confidential information on any Web site if it is not a secure page; look for the image of a padlock in your browser and an address beginning with https://. If you are sharing your computer with anyone else, log out of all secure sites when you are done using them, clear the cache, and close your browser.

Never give out confidential information over the telephone, and never send confidential information via unencrypted e-mail messages—including splitting credit card numbers into multiple messages, because that affords little protection.

Before disposing of any hard drive or computer containing one, delete all of your personal files, empty the Recycle Bin, and then utilize a "wipe" utility to sterilize all of the free space, using multiple passes, even if that requires running the process overnight. Otherwise, thieves and pranksters can recover your "deleted" data because it still resides on the hard drive, even though the files are no longer seen by the operating system.

If you fear that your identity has in fact been stolen, contact the proper authorities. If it involves any financial data, immediately contact those institutions. Note that the Federal Trade Commission (FTC) has information on identity theft (*consumer.gov/ncpw/everyone/identity-theft-and-privacy/*), as does the Privacy Rights Clearinghouse page Identity Theft & Data Breaches (*www.privacyrights.org/identity-theft-data-breaches*).

Most if not all of these security measures can take extra time and effort, but they are nothing compared to the financial loss and sense of violation if and when you fall victim to identity theft. An ounce of prevention is worth a pound of cure.

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

Is Online Shopping Safe?

“Simple safety measures when shopping online.” by Pete Choppin

Online shoppers beware: Thieves and fraudsters would like nothing more than to get their hands on your name, credit card information, checking account number or anything else they can use to rip you off.

I use many online vendors and Web sites for the types of products and services we buy where I work. It has become second nature for me to follow basic safety measures when shopping online.

I am often asked whether online banking is secure, and I generally advise people that doing your online banking and bill paying is generally safe. But it seems that online purchases are decided upon at the drop of a hat, leaving caution to the wind. And why? Because of the allure of shopping from the comfort of your home and receiving your new goods without setting foot in a store.

When you shop online, however, you have to be more aware of thieves and fraudsters who'd like nothing more than to get their hands on your name, credit card information, checking account number or anything else they can use to rip you off.

Fraudsters can get access to your personal information online by setting up fake stores, which can look amazingly similar to the real thing. They may even go so far as to confirm your order and send an e-mail confirmation. However, it's only when you don't receive the merchandise you paid for that you realize you may have been a victim of an online shopping scam.

If you shop online you have to be careful; otherwise, you could find yourself dealing with hundreds of fraudulent charges.

It makes sense that better security often means sacrificing convenience. Open 24 hours a day from anywhere in the world, online shopping sites entice consumers with an array of come-ons, such as free shipping, comparison pricing, bargain deals and extra security features. Saving gas, and being able to shop on your schedule, adds more to the online shopping appeal.

Yet, the question remains: Can online shopping be done safely?

Most experts agree that it can—on the condition that consumers abide by some basic safety tips.

Tip No. 1: Bigger Names Equal Better Protection

"Go with reputable companies you've heard of," says Jim Stickley, co-founder, CTO and vice president of engineering at TraceSecurity, a company

that works with financial institutions to better their network security systems to deter identity thieves.

Stickley, who knows firsthand how easily sensitive information is stolen, says that if a deal sounds too good to be true—say, $20 for an iPod Nano—it probably is. What's worse, it's probably an attempt to trick you into giving out personal information.

Steven Branigan, founder and president of CyanLine and author of *High Tech Crimes Revealed*, agrees and says that it's good to know the site you're going to, such as bigger sites like Amazon.com. "These sites put their name on the line."

On the other hand, the fear factor hurts smaller merchants who might have better deals, which is, of course, immaterial where your security is concerned.

Tip No. 2: When in Doubt, Check Them Out

If you go with an unknown merchant or Web site, contact someone there who can verify the company's privacy policy for you before you make a purchase. Ask if they'll send you a catalog. If they don't list phone numbers and only have an e-mail address, that's a huge red flag. Call the phone number and see if it goes to voice mail. Anyone can have voice mail set up.

Bottom line: If you can't get a human being on the phone or don't like what you're hearing, go shopping somewhere else.

Tip No. 3: Encryption Doesn't Equal Security

Leah Ingram, author of *Gifts Anytime: How to Find the Perfect Present for any Occasion,* is a certified etiquette and protocol consultant. This expert gift-giver says one of the first things you should do before typing in your credit card information is look for the "plural URL." That is, when you go to the site's checkout page, make sure it is a secured Web site by checking for the "https://" in the URL. The "s" designates a secure site. It isn't a guarantee, so also check for a closed padlock or key that should also be on the page, letting you know your personal information will be encrypted or scrambled.

If you don't see either of these "locked" icons or a change in the URL, log out and shop elsewhere. You can't be sure the site has a secure server, and you shouldn't take that risk.

Here's one tell-tale sign that you've entered a scammer's site: If you ever see numbers at the beginning of the URL, such as http://66.102.7.104@65465.51456%6AD%, it's probably a scam, says Stickley.

Even if you see a proof of encryption, such as the plural URL, you shouldn't equate that with the site's trustworthiness.

"It just means the session is encrypted," says Stickley. He likens the mistaken notion to believing that someone owns a house just because that person can lock the front door. It means nothing. To verify the site's trustworthiness, he advises calling the company to ask about its privacy policy.

Tip No. 4: When Sharing Is a Bad Thing

Shared computers, such as the ones available to multiple strangers at computer centers, are a big security risk.

The danger is that hackers can insert a keylogger into the back of the keyboard, a device that looks like a harmless adapter. This monitoring device captures everything you type before it's encrypted. Sometimes installed as software, the device can be hard to detect. The best thing to do is avoid shared computers when typing sensitive information.

Tip No. 5: Pay With a Credit Card

You've found a trustworthy site with a secure checkout page. Now you're ready to pay—with what? Check, money order, debit card, credit card, cash or Monopoly money?

Experts all agree: Credit cards are the safest method for online purchases.

Personally, I hate credit cards. I don't carry any. And although this flies right in the face of expert advice, keep in mind that I am very careful about where I purchase online. I scrutinize every site and I would never hand over a debit card number to a site I didn't know and trust.

However, it is good to know about some of the security protections that credit cards provide.

"The last thing you want to use is a debit card," Stickley says. "Most credit cards have protection on them—if someone rips you off, you can dispute the charge. Debit cards pull money right from your bank account. It can take months to get your money back, if you ever see it again."

The advantage of using a credit card is that it's not just your money on the line—it's the creditor's money, too. If you have a problem with your transaction, the credit card company will go to bat for you to resolve it because, in the end, the creditor has just as much at stake as you do.

Another option is making purchases through a third-party escrow service such as PayPal. PayPal Buyer Protection covers qualifying eBay purchases for up to $1,000 at no additional cost to buyers, helping to guarantee your purchase. After any sale, be sure to print and save all of your receipts and e-mail confirmations in case of a dispute.

Credit shy?

If you are understandably reluctant to give out your credit card number over the Internet, you have alternatives. Some card companies such as Discover Card, Bank of America and Citi, offer a secure online account number service—a virtual credit card or virtual account number.

By providing merchants with a special credit card number instead of your real number, your actual Discover account number is never exposed to scammers. Check with your credit card company to see if it offers this type of security feature.

Another security feature on the horizon is a one-time-use password token. The technology has been developed, but it's not in widespread use yet. To protect yourself, be wise in your choice of passwords. Use a combination of letters and numbers difficult to guess. Don't use a word or number someone else could figure out, such as your birthday or dog's name. Change your password frequently.

Tip No. 6: Suspect the Suspicious

If you're at the checkout page and the site asks for your date of birth and Social Security number, be very careful. This kind of information can give people enough to start applying for new credit cards in your name. What's scarier is the ease with which driver's licenses can be purchased overseas (*www.consumertraveler.com/today/beware-fake-international-driving-permits/*). If that scares you, remember a simple rule of thumb: If anything seems suspicious, call the company and ask questions.

Also be wary of sending out credit card information via e-mail or instant messaging—neither is encrypted. Copies can remain on your mail server as well as theirs. Since you can't control who's looking at your information, stick to the site's secure transaction page.

The Final Word

The experts offer a silver lining to the cautionary warnings against online identity theft and credit card fraud. People should be aware that as long as they are dealing with reputable companies, online transactions are far more secure than the face-to-face transactions people perform every day.

Online transactions eliminate the middle man, such as the waiter who processes your credit card payment, so there are less people who physically see your private information.

Consumers who research companies before making purchases, watch for warning signs of fraud, use credit cards for purchases and keep receipts should be relatively safe.

"They can be absolutely as confident as physically shopping in a store," says Stickley.

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

Windows Tips and Tricks

Windows Media Programs

“Creating a Windows PC TV” by Jack Dunning

As we take a closer look at Windows media programs and how they work together, it's time to turn our computer into a broadcast television set.

As we take a closer look at Windows media programs and how they work together, it's time to turn our computer into a broadcast television set. If you want to save the cost of a cable television bill, then broadcast TV remains a viable alternative as long as you live in an area with decent reception. Not only are there still many stations that can be picked up over the air, they seem to be multiplying—at least from what I can remember. It's been decades since I've hooked up an antenna to a television, so this was a little bit of an eye-opener.

To make your Windows computer into a television, you need a receiver that can tune in the local stations. That may be in the form of an expansion card or a USB device. I decided to go with the Haupauge WinTV-HVR-950Q Hybrid TV Stick (*www.hauppauge.com/site/products/data_hvr950q.html*) (price $75-$80), which is USB. The advantage to a USB device is that it's easy to move to a different computer and take with you if you're traveling. This could be a great advantage if you want to watch something other than SpongeBob SquarePants when visiting grandchildren. It may not be a good choice if you have a limited number of USB ports, since it's not recommended that it connect via a hub.

My goal is not to watch television on the computer, but to stream television from the Windows 7 computer to the main television. My research tells me that there are a number of things that need to be put in place—the first being the programming itself. The USB television receiver can provide the television programming to the computer. The next stage will be sending the content from the computer to the television. I don't need a TV receiver to stream content to the television. I should be able to send MP4 files and other media available over the Internet as long as I have the proper hookup at the television set. But that process I'll address in future columns. For now I'll be happy to tune in some local broadcast television stations.

The WinTV USB device was fairly easy to install. It came with its own software for detecting signals and adding them to a list of local stations. It can either be used for the digital antenna signal (ATSC) or unencrypted digital cable (QAM). It doesn't take long to determine if it will work for your computer and your location. While the device comes with an antenna, unless you're perched at an optimum antenna location, you will probably need something more for better reception. The second floor will be better than the first and the rooftop will be best of all. Also, the

bigger the antenna, the better—it's simple wave physics, which haven't changed in the digital age.

Signal reception is far more important than the speed of your computer. If you have a poor signal, the problems will look similar to slow computer issues. The picture—if you get one at all—will experience pixilation and freeze up. The audio may continue or cut out much as it would if you were experiencing slow decoding of the signal. But the problem is probably not the computer, but rather the signal strength. If you live in an area with weak television signals, then attempting to bring a broadcast signal to it may not be worth the effort or price of the receiver.

Once the receiver is installed and at least picks up a station or two, then it's time to set it up with Windows Media Center. Remember that Windows Media Center is aimed at turning your computer into a television whether the programming comes from a DVD, a receiver, or the Internet. Windows Media Player is a controlling and playing program for all types of media except (as far as I can see) some of those supported by Window Media Center, such as live television and Internet programming.

Once the television receiver is installed and the Windows Media Center is loaded, the steps for setting up live TV are initiated by selecting "live tv setup" from the TV category. (These steps refer to setup in the Windows 7 version of Windows Media Center.) Once live TV is set up, the words "live tv" will appear in the TV menu. If the receiver is not detected by Windows, the setup procedure will not continue. The first screen will ask you if you want to configure for your current location or another geographic area (see Figure 1). On the next screen you will enter the local ZIP code

Figure 1. Configure for the local geographic area.

At some point, the wizard will query which type of service you want to download. Generally, you will have a selection between local cable companies (QAM) and a digital TV antenna (ATSC). Unless you are hooking up unencrypted cable, select the antenna. After installing Play Ready software, the programming for your local area will be downloaded. The most time-consuming portion of the process will be the scanning for signals (see Figure 2). Be patient.

Figure 2. TV Channel Scan in Windows Media Center.

Once the process is complete, you will see the channels added to the programming schedule, which includes the offerings from Internet TV (see Figure 3).

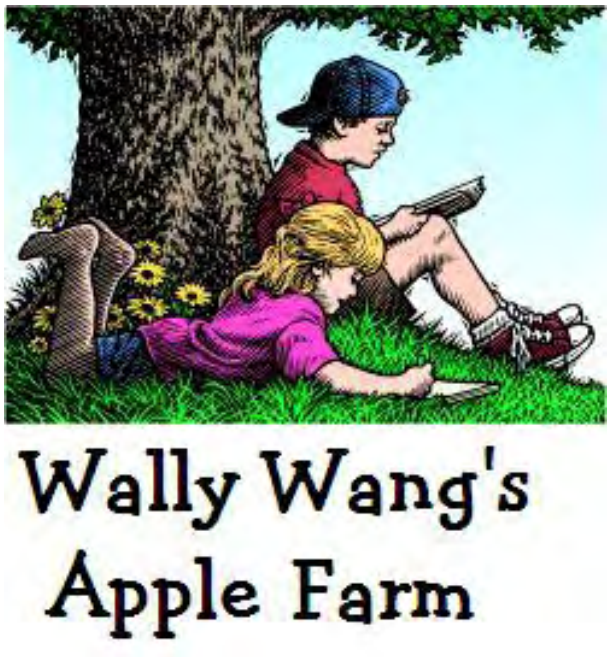
Figure 3. Live broadcast television programming added to Windows Media Center.

If you have poor signals for some of the channels, they most likely get no picture. There are tools to isolate the good signal channels, but that is a question for next time. For now you can click through the channels and see which will connect for you. If it works, you will get something similar to Figure 4.

Figure 4. Live antenna broadcast television playing in Windows Media Center.

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



Wally Wang's Apple Farm

“Security on the Internet” by Wally Wang

Simple precautions help you safely navigate the Internet without losing money to criminals. Also, people criticize Apple without first investigating the facts; InDesign now offers collaborative features; Bento is a deceptively simple yet flexible database program; and a tip on double-clicking on the title bar of a window you want to temporarily hide.

Many people are concerned about security over the Internet, fearful of hackers breaking into their computers and stealing their credit card numbers or Social Security numbers. While it's possible that hackers could target your computer, the truth is that hackers are just one of many ways you could lose your personal data.

Hand your credit card to a waiter or waitress in a restaurant, and that person could write down the numbers and use them. Check into a hotel and use a credit card to charge your room, and the hotel workers can snare your credit card number. Even if you never let your credit card out of your sight, someone back at the VISA, MasterCard or American Express offices can always get access to everyone's credit card numbers, so you have to trust that some disgruntled worker won't take advantage of this access and steal your credit card number.

While many people protect their data from thieves, they then use social networks like Facebook and LinkedIn to reveal sensitive information about themselves. Burglars regularly scan social networking sites to find when people will be on vacation (so they can break into an empty house), and identity thieves scan sites looking for clues that can help them gain access to passwords and accounts, such as people listing their favorite colors, pet names, or family tree (which can reveal their mother's maiden name).

Credit card fraud is impossible to stop, but you can still minimize your risks. First, consider dedicating a single credit card to online purchases. That way if something suspicious appears on any of your other credit cards, you'll be able to spot the problem right away.

Second, shop online through trusted retailers such as Amazon.com or other larger retailers. Buying online through a small, unknown retailer simply increases your risk by exposing your credit card data.

Third, make sure that whenever you shop online you use a secure connection. This simply prevents any sensitive data that you type from being stolen as it's sent from your computer to the retailer's computer. The risk of someone snaring your credit card data as it's being sent is small,

but it's a risk you never need to take.

On Safari, there are two clues to show when you're securely connected to a Web site. First, look in the address bar for "https://" in the first part of the address (which stands for HyperText Transfer Protocol Secure).

Second, look for the lock icon in the upper right corner of the Safari window. If you see both this lock icon and the "https://" portion of the address displayed, you can be sure you're securely connected to a Web site. (Now whether that Web site itself is secure is an entirely different story.)

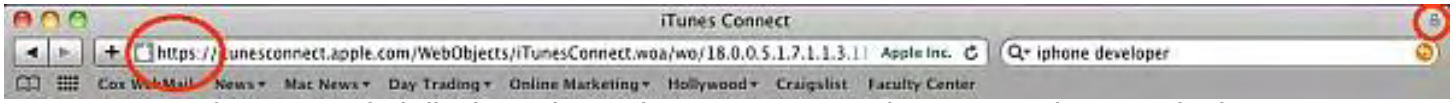


Figure 1. Safari displays clues when you're securely connected to a Web site.

Finally, be careful what you post online that others can read. You don't want to give identity thieves personal information that they can use against you. All of these precautions can't keep you 100 percent safe, but it can go a long way toward reducing your risks so you can safely navigate the Internet without losing money to criminals.

The Fear of Change

A friend of mine recently asked his IT manager about the possibility of switching from Microsoft Exchange server to Snow Leopard server. Immediately, his IT manager produced horror stories of incompatibilities and the high cost of Snow Leopard Server. The problem with all of his arguments was that they were completely wrong.

Snow Leopard server costs only $499 vs. $699 for Microsoft Exchange Server, so while the capabilities of each may differ, the cost alone is actually in favor of Snow Leopard server. The horror story of incompatibilities also proved incorrect because Snow Leopard server can work just fine in a mixed environment of Macintosh and Windows PCs.

The problem wasn't that the IT manager looked at the needs of this company and objectively concluded that Microsoft Exchange server was the better option, but rather that he simply rejected Snow Leopard server without learning anything about it first. Perhaps if he did take the time to learn the facts, he wouldn't like what he would find out. Rather than deal with reality, he preferred to ignore it and and convince others to ignore it as well.

Of course, if my friend's company does switch to Snow Leopard server, this IT guy has only Microsoft Exchange server skills and would thus be out of a job. This self-preservation instinct appears to be the primary reason why so many people immediately dismiss Apple products without bothering to learn the facts, in hopes that others will accept their conclusions also without checking the facts.

Roger L. Kay of Forbes recently wrote an article criticizing Apple (*www.forbes.com/2010/07/07/apple-fires-customers-intelligent-technology-iphone-ipad.html*) for not supporting blind users and for not supporting the Chinese market. Within hours, Forbes had to retract Roger's statements about the lack of support for blind users because his criticism was completely wrong.

Apple offers VoiceOver (*www.apple.com/accessibility/voiceover/*) for reading screens to blind and low-vision users. Although the iPad may only present a smooth surface, Apple includes features that can read to blind users so they know what their fingers are touching on the screen, making the iPad completely accessible to blind users (*www.associatedcontent.com/article/2859598/ipad_review_from_a_blindness_perspective.html?cat=15*).

Rather than simply visit Apple's Web site or even try an Apple product for himself, Roger L. Kay spouted off pointless criticism to tear down Apple, which basically revealed both his ignorance and his bias against Apple.

Although Forbes corrected Roger's column regarding blind users, it still left behind Roger's other criticism that Apple isn't adopting its products for the Chinese market, which again is completely wrong.

The iPad lets users type Chinese characters through an ordinary keyboard (a method called Pinyin) as well as including character recognition, so you can draw a Chinese character with your finger and the iPad displays a list of characters that it thinks you want to write. Then you just have to tap the character you want.

Figure 2. The iPad offers a Chinese character-recognition feature..

Mac OS X also supports this same Chinese character-recognition feature on laptops. Just trace the Chinese character on the trackpad and Mac OS X displays a list of Chinese characters it thinks you're trying to write.

Figure 3. Mac OS X supports Chinese character recognition on laptops with a trackpad.

So not only was Roger L. Kay completely wrong in stating that Apple doesn't offer features to assist blind users (which Forbes retracted), but he's also completely wrong about Apple not providing features for the Chinese market (which Forbes has yet to retract).

Perhaps the following statement by the German philosopher Arthur Schopenhauer explains why so many people criticize Apple without first investigating the facts.

"All truth passes through three stages. First it is ridiculed. Secondly, it is violently opposed. Third, it is accepted as being self-evident."

When Apple first released the iMac, iPod, iPhone and iPad, many people ridiculed them as failures. When these products succeeded anyway, these same critics violently criticized them using fiction and distorted truth.

People fear and resist change because change requires learning new skills and starting all over again as a novice, essentially dumping years of hard-earned previous experience down the drain. When Microsoft tried shifting everyone from MS-DOS to Windows, many people violently opposed this shift to Windows. When the computer industry shifted from WordStar to Word Perfect and then to Microsoft Word, people fanatically stuck by their favorite word processor and resisted change. When the operating system market shifted from the then-leader CP/M-80 to MS-DOS, technical people criticized MS-DOS as a "toy" operating system and a limited imitation operating system while promoting CP/M-80 as a "business" operating system. Sound familiar?

InfoWorld

for the busy manager. (9/9/85)

HP Tape Backup 9142A *(Hewlett-Packard)* — Oversized, expensive, and slow in operation, Hewlett-Packard's 60-megabyte tape backup unit is hampered by flawed documentation. Once the obstacles are overcome, it delivers satisfactory performance. (10/21/85)

IBM Color Jetprinter *(IBM)* — The IBM Color Jetprinter is a great buy. It produces sharp color graphics and uses easy to load and clean ink-jet cartridges. The printer even comes with software drivers for popular programs such as Lotus' 1-2-3. The trade-off is that it's quite slow. (9/2/85)

Mac Charlie *(Dayna Communications)* — Mac Charlie is a box that adds true IBM PC monochrome compatibility to the Macintosh. Only time will tell whether this concept is brilliant or crazy; at this time, the system shows tremendous promise but is still having substantial problems, including erratic performance in the critical key data transfer area. (9/16/85)

Macmodem *(Microcom)* — The Macmodem is easy to use and ideal for beginners. It performed well in all our tests; however, the price is high compared to many other 2,400-bit-per-second modems on the market. (10/7/85)

Maxwell Modem 2400V *(Racal-Vadic)* — The Maxwell 2400V is a quality product at a fairly low price, but this modem is best suited for experienced users. (10/7/85)

Morrow Pivot II *(Morrow)* — Eminently portable and with an exemplary LCD screen, the Pivot II would be worth considering as a lightweight portable, except for unresolved problems with a failing battery. (9/23/85)

Panasonic Executive Partner *(Panasonic)* — This is a transportable MS-DOS computer with a built-in thermal printer and a light emitting plasma display. The built-in thermal printer may be attractive to those who need on-the-road draft printing, but setup seemed to require three hands. (9/23/85)

PC Turbocharger *(Univa-*

Review Responses

PANASONIC'S NO HEAVY

In the review of the Panasonic Executive Partner ("Panasonic Executive Is Reliable Partner," September 23, 1985), you mentioned that the earlier Senior Partner weighs over 40 pounds. The Senior Partner's two-drive floppy system weighs less than 30 pounds.

The reviewer had difficulty using Dbase III, Version 1.0 on the Executive Partner. Try the current version of Dbase III, Version 1.1, and you will not have any problems running at either fast or slow clock speed. The older version of Dbase III, Version 1.0, had some bugs in it.

R.D. Scobee

CP/M PREFERRED

I take exception to your review of the Bondwell Portable ("Bondwell's Laptop, Limited, But Cheap," October 7, 1985), not so much for [the criticism] of the machine itself, but for the criticism of the CP/M operating system. I have had a Kaypro 2 for about a year. I have not been disappointed. The software that came with the machine has proved an invaluable tool in my computing education. The whole idea behind a CP/M laptop is portability. Laptops should not be considered a primary computer. Thus, it is not surprising that a CP/M laptop is being offered to the large audience of CP/M users.

I like CP/M. It is much more efficient than MS-DOS. (Ever wonder why MS-DOS programs cost more and require more memory than their CP/M counterparts?) CP/M is capable of color with the addition of a color board from any of the various manufacturers. There are many new software and hardware products available for CP/M and more coming out every month. There are even programs that work like Borland's Sidekick for CP/M.

Another advantage of CP/M, which I find rather important because it is what most people buy computers for, is that it requires no special board for doing advanced math processing as do MS- or PC-DOS operating systems.

The lowly 8-bit, Z80-based microcomputer can be set up with 256K of random-access memory (RAM), multiuser capability, 1 megabyte or more of RAM disk, a 10- to 40-megabyte hard disk, and a clock speed that will put most MS-DOS-based machines to shame — and for much less than the price of a new PC XT or PC XT clone (which would be comparable to the above). With all that, who needs windows?

Don't ignore or write off CP/M. While you were not looking, many things have been happening. Your MS-DOS is rapidly becoming the slow kid on the block!

Guy Pace
Ellensburg, WA

NOT IN THE IBM CAMP

I am a new subscriber to *InfoWorld*. After two issues, it appears to be useful. It would be much more so if the evaluations included the suitability of any software for use on non-IBM micros.

For instance, Word Perfect from SSI is an excellent program and a version for the Texas Instruments Professional is available. That is not mentioned in the review. Rbase 4000 runs on the TI Pro in the IBM emulation mode with no problems. I have both an Apple and a TI Pro that are used in my firm. I'm beginning to wonder if I should stop fighting it, trash the non-IBM machines and go buy an IBM. As long as the usability of the programs as reviewed is restricted to IBM and "compatibles," *InfoWorld* seems to be promoting the myth that there is only one brand. Is that true?

Bob Johnson
R.C. Johnson and Associates
Everett, WA

Versions of software products are so numerous that our reviews can't, as a practical matter, exhaustively list all of them; query the vendor regarding specific systems if necessary. Our attention to IBM PCs and compatibles reflects not promotion but the reality of our readers' configurations: IBM and close compatibles account for the bulk of MS-DOS computer sales. — Editors

---

InfoWorld *welcomes comments about its reviews. Letters are subject to editing for space and clarity. Please address correspondence to the Review Editor,* InfoWorld, *1060 Marsh Road, Suite C-200, Menlo Park, CA 94025.*

Figure 4. The October 28, 1985 issue of InfoWorld contains a letter from a CP/M-80 user, criticizing MS-DOS.

Rather than adapt to change, some people violently oppose it without even realizing that what they're defending as self-evident was once violently opposed by others in the past. Now as the era of Windows dominance begins to fade, there will be those who simply refuse to acknowledge anything positive about Apple products. Eventually when the world shifts away from Windows, these same people will likely grudgingly accept Apple's influence and then suddenly defend their choice of Apple-influenced products as if it were self-evident that they recognized the benefits of Apple's products all along.

Then when the next wave of change hits the computer industry, these same people will violently oppose any change, rely on ignorance and out-of-context facts to maintain their delusions, and continue the cycle all over again. History really does repeat itself.

Collaborating with Adobe InDesign

Adobe's InDesign is rapidly becoming the standard desktop publishing solution. However, designing pages in InDesign is rarely a single person effort. Instead, multiple people may need to collaborate and review an InDesign document.

If you're ever collaborated with Microsoft Word documents, you know how to track any changes that different people make. Now InDesign offers this same tracking feature as well so you can not only see changes made by multiple reviewers, but selectively accept or reject them.

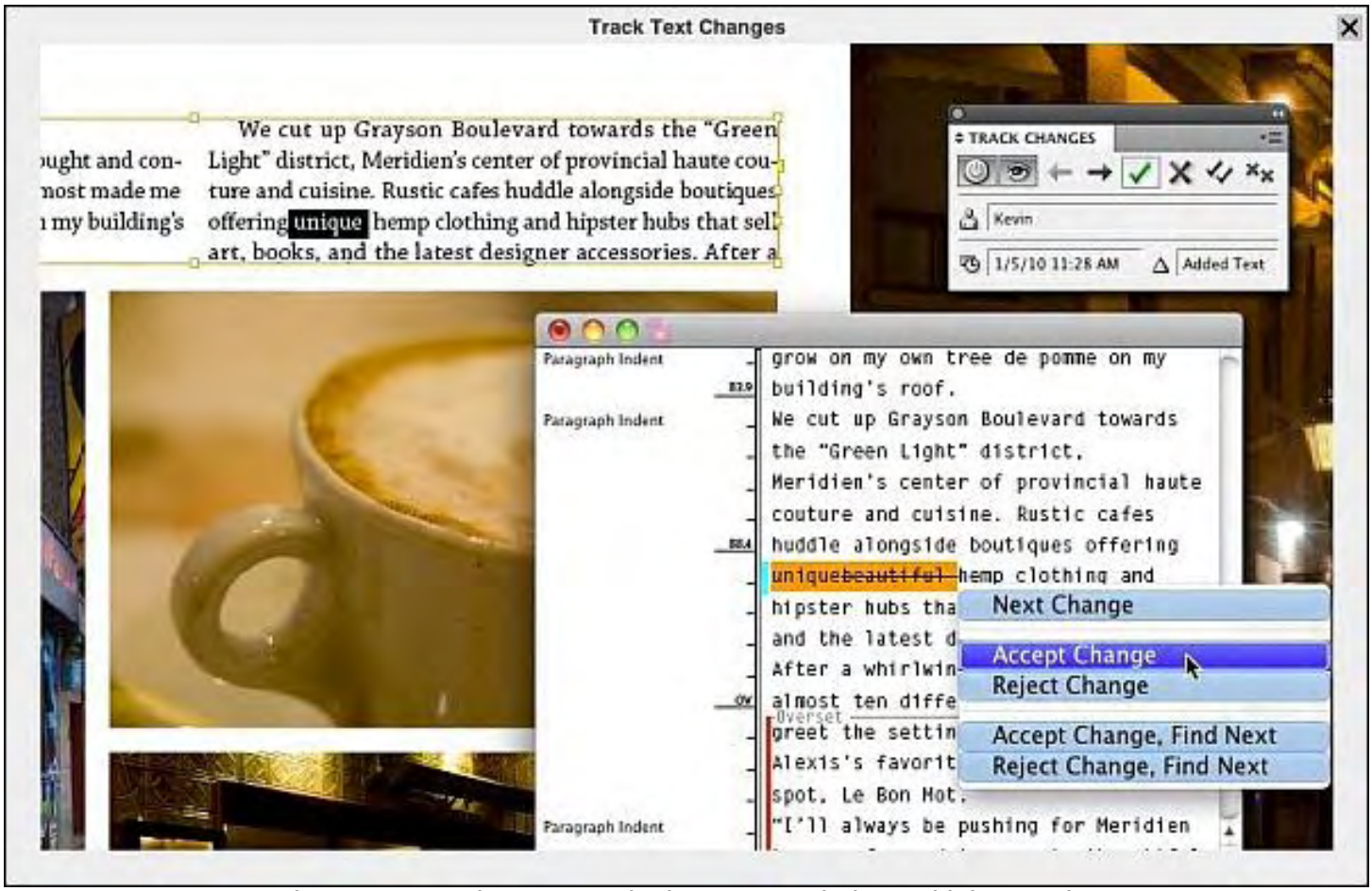


Figure 5. InDesign can track changes made by multiple people.

Bento Templates

One problem with database programs is that they're either too powerful (and complicated) or too simplistic (and limited). Every Macintosh comes with two simple database programs called Address Book (for storing names) and iCal (for storing appointments), but storing information in two separate programs can be clumsy.

To solve this problem, get Bento (*www.filemaker.com/products/bento/features.html*), a simple

$49 database program that can automatically access any data you've already stored in Address Book or iCal. Make changes in Address Book or iCal and those changes automatically appear in Bento because Bento simply loads data from both programs without duplicating it.

Besides letting you access your Address Book and iCal data in one place, Bento also lets you use templates for organizing certain types of data, such as its free Student Survival Kit template (*solutions.filemaker.com/database-templates/detail.jsp?serial=2551644*). Anyone going to school might find Bento's lecture notes template handy for keeping class notes organized.

Figure 6. Bento offers a student survival template for organizing class notes.

For anyone looking for a job, use Bento and the free Job Hunting Template (*solutions.filemaker.com/database-templates/detail.jsp?serial=2550208*) to help organize your job search.

Bento is a deceptively simple, yet flexible database program that you can easily modify using numerous free templates. If you just need to store data and don't want to wrestle with more complicated database programs, Bento may be the program that could solve your problems.

* * *

If you want to tuck a window out of sight temporarily, you could click the yellow button that appears in the upper left corner of every window. However, a faster method is to double-click on

the title bar of the window.

Either method shrinks your window to the right side of the Dock near the Trash icon. To open this window, just click on its icon on the Dock.

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 2010 for Dummies (*www.amazon.com/gp/product/0470489987?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=0470489987*),
Beginning Programming for Dummies (*www.amazon.com/gp/product/0470088702?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=0470088702*),
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*),
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*),
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*),
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*),
My New iPad (*www.amazon.com/gp/product/1593272758?ie=UTF8&tag=the15minmovme-20&linkCode=as2&camp=1789&creative=9325&creativeASIN=1593272758*),
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*),
How to Live With a Cat (When You Really Don't Want To) (*www.smashwords.com/books/view/18896*).

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

Rob, The ComputorTutor: Tech Solutions with Microsoft Word

“Word Labels” by Rob Spahitz

We've now finished our awesome resumes and made some terrific business cards. Now we need to mail them out, and we want the envelopes to look professional.

We've now finished our awesome resumes and made some terrific business cards. Now we need to mail them out, and we want the envelopes to look professional. So rather than hand-print, let's generate them on the computer.

There are a variety of ways that we can make labels and a whole set of issues that come with them.

First, when you create labels, you have to decide where they will print. Do you want to print them on an entire sheet of letter paper, one per page? Of course not! The page is too big. You could print directly onto the envelope. If you have your own personal printer, rather than a shared printer, that's probably OK, especially since most printers these days have page-feeders where you could feed an envelope. You could also do that on a shared printer, but then you have to figure out how to get the printer to wait until you load an envelope.

Some actually handle that, so that if the print is set to manual feed, it will wait for you to insert paper into a special paper feeder. As long as you don't wait too long, other people can tolerate waiting for you to head down the hall to that printer and manually feed your envelope while the printer holds onto the "job" that will print your envelope and all of the other jobs queued up waiting to print. If you wait too long, someone may cancel your job or simply feed some standard paper in to get the job printed—and then you'll get your printout on a standard page. Of course, you can also print on a special label-maker printer that is designed to print labels one at a time.

Let's explore these options.

Label-Makers

You've probably seen advertisements lately for special printers designed to print some of the lovely pictures you've taken with your digital camera. These are designed to print on special paper that matches the size you'd expect for a printed photograph. Well, before those were invented, they had the same thing for labels. These were typically designed to produce black images either on rolls of paper, folded sheets of paper or even small individual sheets. There were usually two types: ink printers (like most standard printers, using either ink or sometimes toner), or thermal printers that used heat to burn an image onto special paper.

These were usually very portable devices. They were designed for small jobs, so they could be easily transported, although that was not their main use. However, since they were small, and somewhat expensive, people in offices usually shared them by moving them from computer to

computer as needed.

They also came in a variety of sizes. Some were designed to handle standard mailing address labels (usually one-inch high and a couple of inches wide), while others were designed for printing special barcodes (in addition to text) that could take up a quarter of a standard letter page.

Finally, the paper used in these devices was obviously special size. They often came in rolls that either had labels lightly glued onto them, had that special thermal paper either with or without perforations, or they came in piles of "fan-fold" paper that had perforations at the folds and held either one or two labels in sequence.

If you have one of these printers, it probably has special software to let you print those labels. It may also have a special Word template that lets you use your word processor to set up labels that will fit and print properly on that printer. If you have that printer, you probably don't need today's article, since you're ready to go.

For the rest of us, or if your printer is broken and you still have that label paper, let's see more options.

Direct Print

As mentioned, your printer probably lets you print directly on an envelope. However, most envelopes are not the same size as standard paper, so you either have to guess how your printer will print on a non-standard-size page (and maybe waste a few envelopes along the way), or you can get your word processor to help you out.

First, note that envelopes also come in a variety of sizes. You could look at the box they came in to see if that helps, or just get out the old ruler and measure. I'm looking at one that I think is the standard envelope for sending out resumes, and it's about 9-1/2 x 4-1/4 inches. I can set up my page in Word 2010 to match that, and then set up my mailing address and print, which we'll do next.

The other envelope you might find is the return envelope. These are the ones that fit inside standard envelopes and are used to send a reply back. Often these are pre-addressed or have an open window where you can print on a piece of paper and make sure it shows inside the window. If you have a standard blank one, it's probably about 9 x 4 inches. Be careful with these because a two-page resume, when folded, gets thick enough that it's hard to squeeze it into this envelope.

OK, let's set up for a standard-size envelope.

Open Word 2010 and create a new document using menu tab File/New. Then select the Envelope folder icon. When this connects to the Microsoft server, it will return a collection of envelope templates ready to go, as seen in Figure 1.

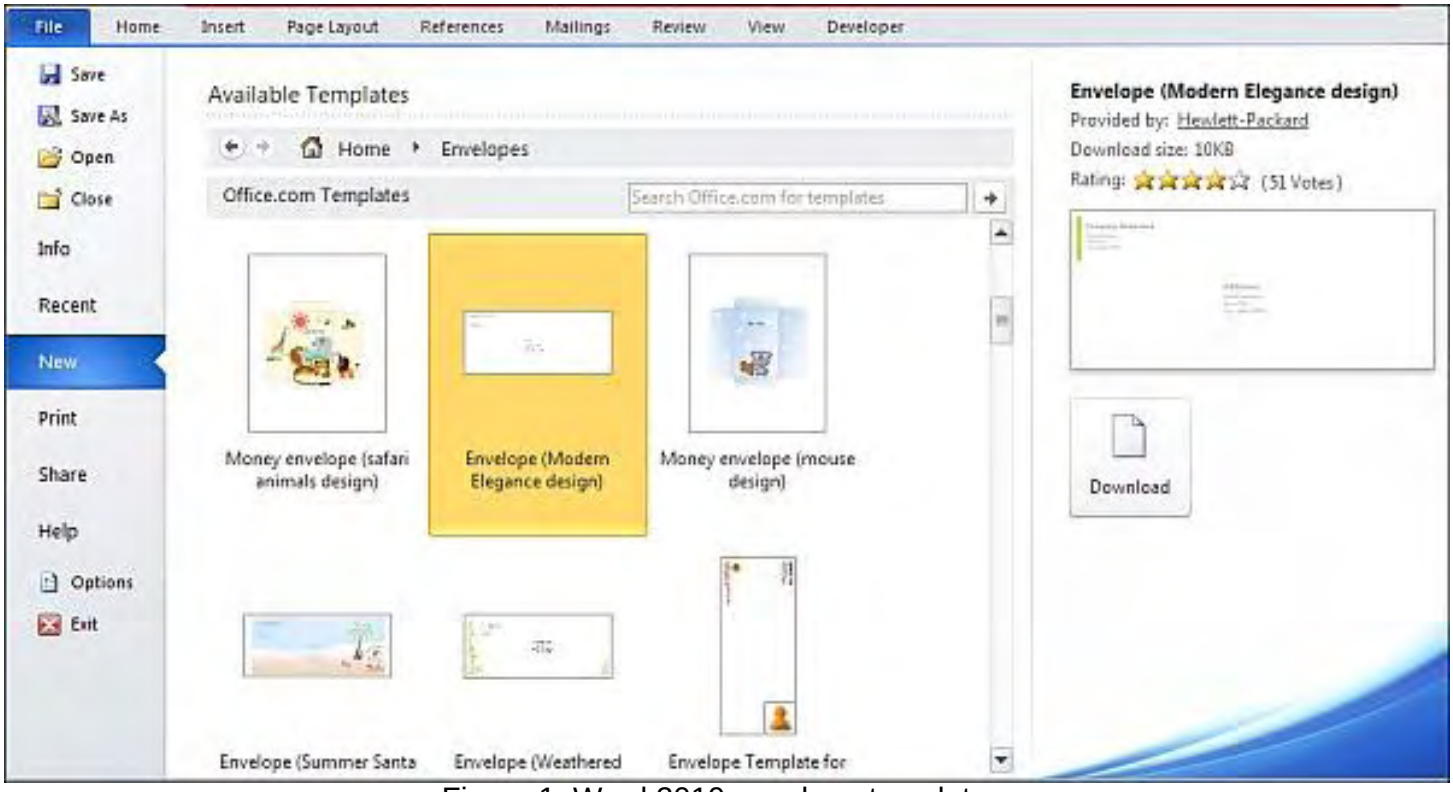


Figure 1. Word 2010 envelope templates.

I'm going to choose the "Modern Elegance design" because it looks plain. If you want a fancier once, pick one that looks good for a resume or business card.

After selecting your choice, click on the Download button in the right panel. When done, you should see something like Figure 2. Note that mine showed up at 125% zoom so I lowered that to 80% by clicking the little "-" near the bottom right corner of the application.

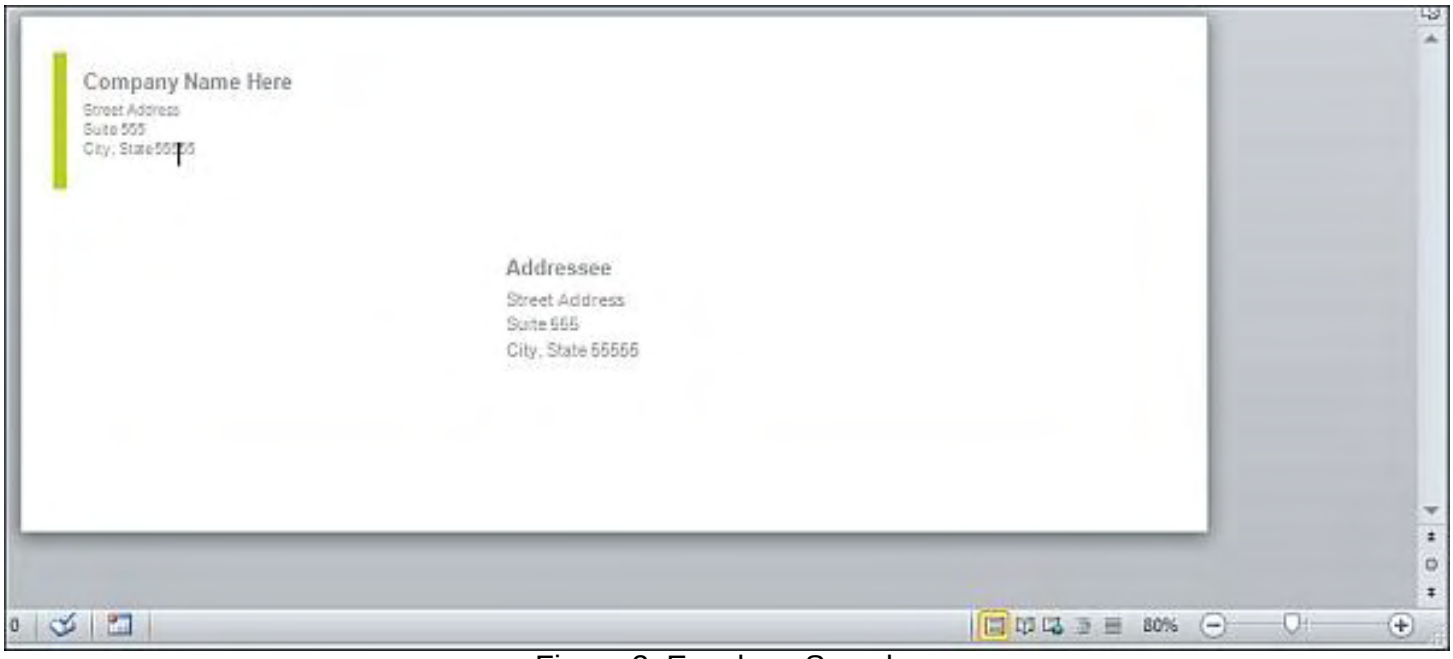


Figure 2. Envelope Sample.

With this in place, type the return address in the upper left corner. Then fill in the person or

business where you are sending this. Next, use File/Print and check the preview window on the right to see if it looks good. By default, this will print in landscape mode (sideways), but if you want to be sure, go to the bottom of the settings section and click on the small Page Setup link, as seen in Figure 3.

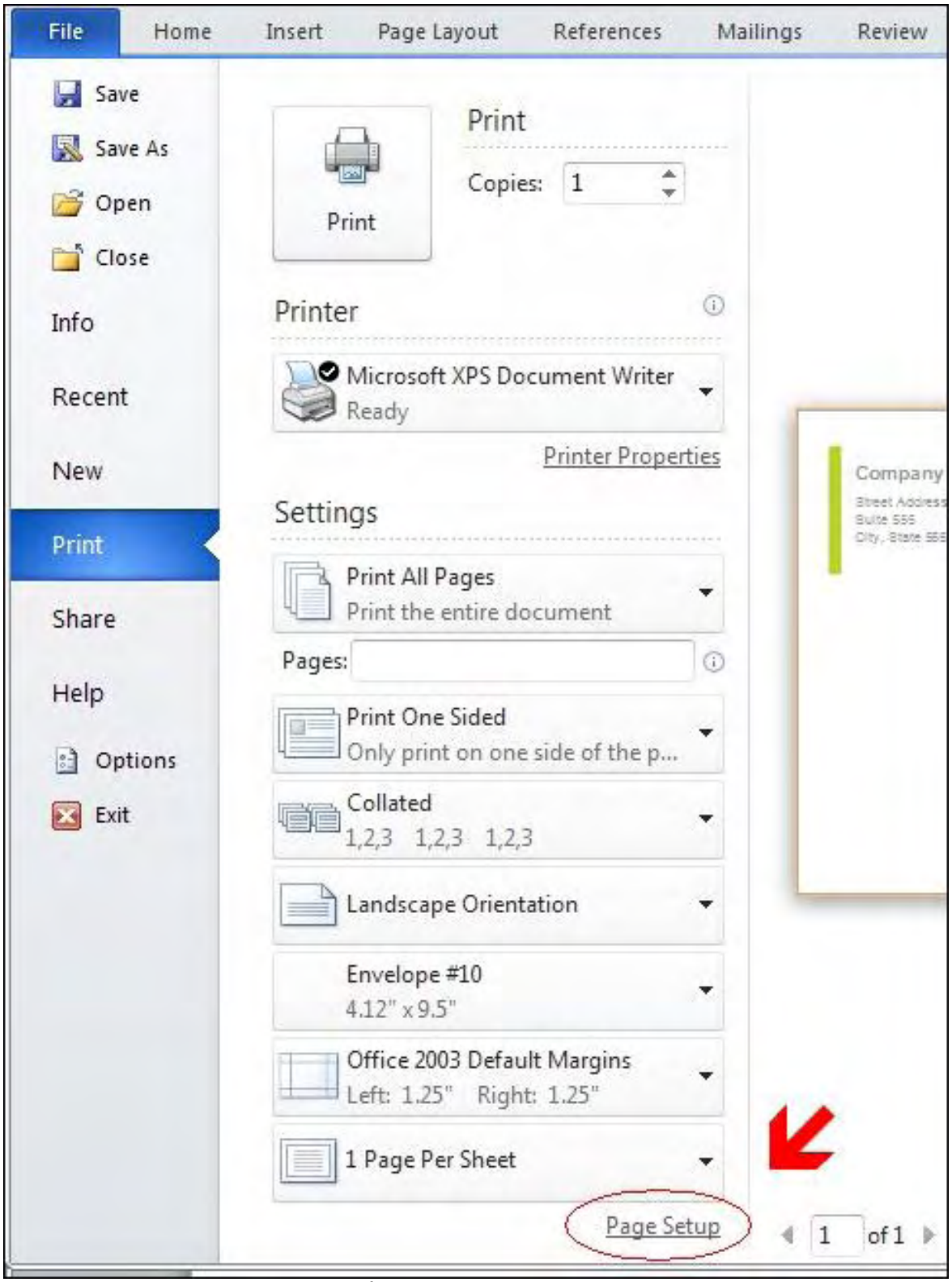


Figure 3. Page Setup.

You'll see a collection of common settings for the page, as seen in Figure 4.

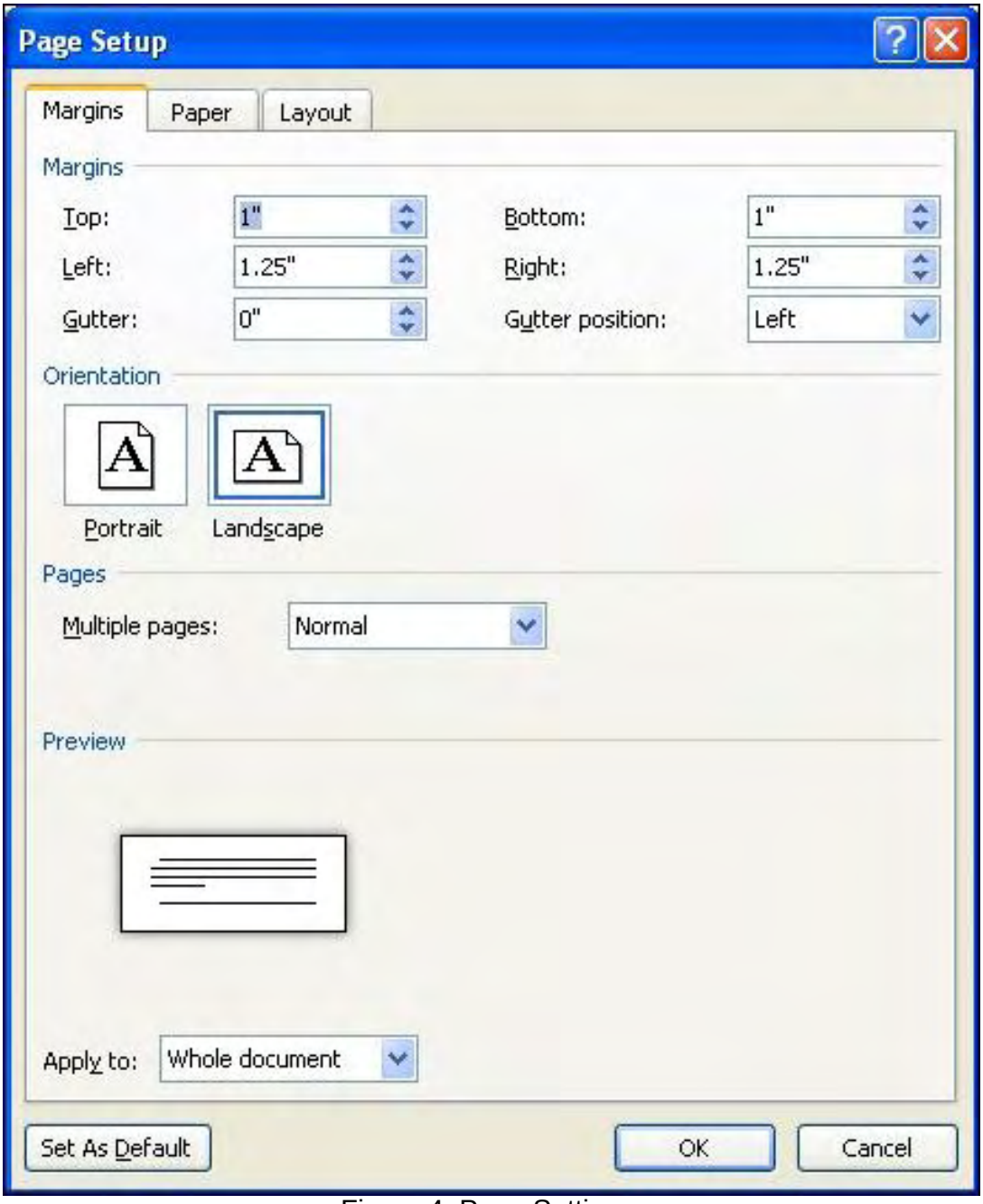


Figure 4. Page Settings.

Obviously, we don't need these here, but we'll change them when we create our own custom envelope.

Click the OK button to save settings or Cancel to retain the current settings.

Back on the main Print page, place your envelope into your printer's manual feed area, usually face up with the flap on the right (but that would depend on your printer) and click the Print button. Note that if you're not sure about your printer's feed style, try using a standard page folded in half to see where the print ends up. Just make sure you remember which side you fed in. You may want to mark one corner with a pen first. Also note that many printers let you adjust the manual feed slot to match the paper size. Since you probably want the envelope centered, adjusting the paper width will help to center the envelope before you print.

When printing labels, one of the toughest parts is knowing how your printer will print. Since printers all work a little differently, I suggest experimenting first, and then making a note (on a sticky paper?) to yourself about how to align the envelope and tape the envelope to the front or side of the printer for future reference. Something like "envelope face up, opening on right" could do it, or even a little drawing that helps you.

Let me know how that works for you.

Since we're just about out of space today, let me wrap things up. When you need to print envelopes, you can find yourself a separate label-maker, but that costs extra money. If you don't plan to print too many labels, your money is probably better spent elsewhere. Your printer can probably feed an envelope in through the manual page-feed slot, but you'll have to ensure that it prints the proper way on the envelope, so try a sample page first. You could also try inserting it into the paper tray, but I'd guess you'd have about an 80 percent chance of a paper jam or misfeed. So for the remaining cases, let's print labels on a standard-size sheet. We'll look at that next week.

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

Worldwide News & Product Reviews

“The latest in tech news and hot product reviews.” by Charles Carr

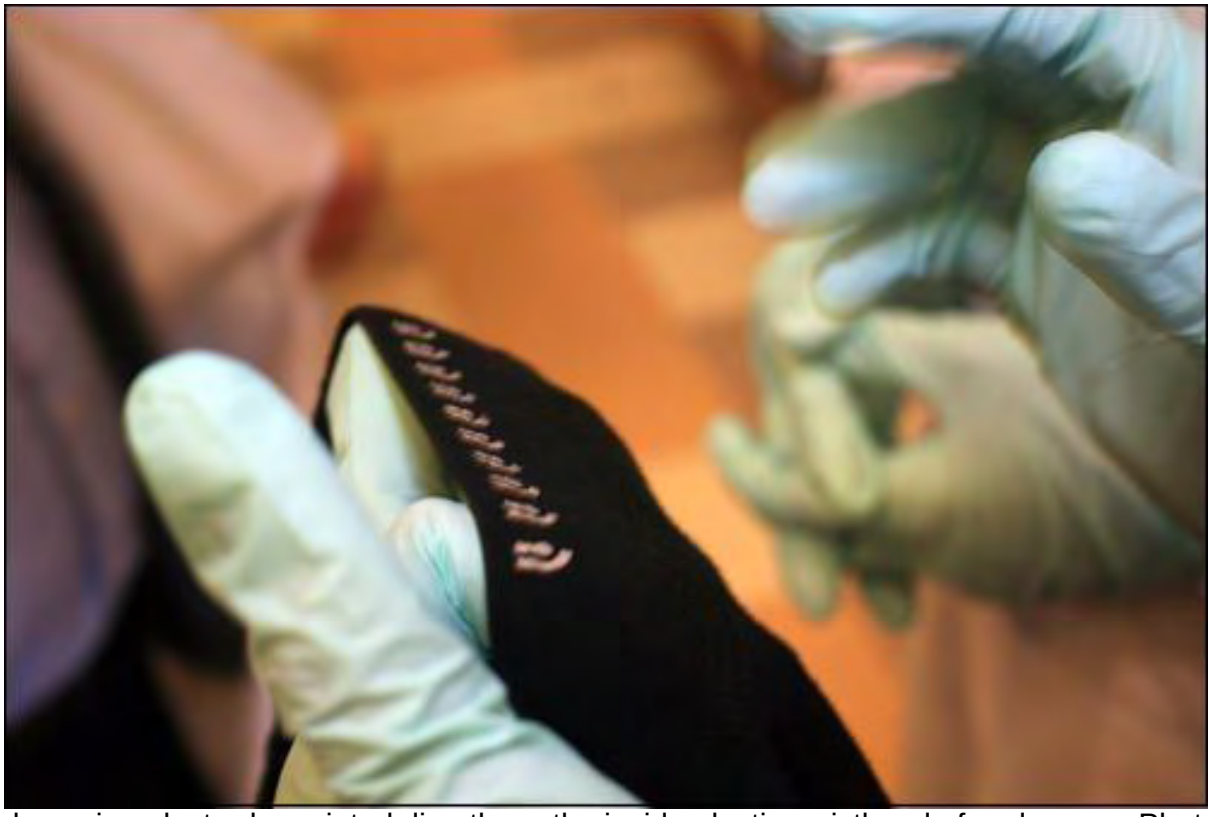
Is Your Underwear As Smart As It Could Be?—Sensors will be incorporated into logic-based biocomputing systems to monitor biomarkers; iGo Green Laptop Travel Charger: One Less Vampire in the House—Uses less than 15 percent of the standby power of standard chargers; Your Vest Friend When Traveling—A look at SCOTTEVEST's gadget-lovers' garments.

Is Your Underwear As Smart As It Could Be?

According to info from the UC San Diego Jacobs School of Engineering:

Chemical sensors printed directly on elastic underwear waistbands retained their sensing abilities even after engineers stretched, folded and pulled at the chemical-sensing printable electrodes—sensors that could one day be incorporated into intelligent "hospital-on-a-chip" systems.

The goal of a peer-reviewed study published in the journal Analyst was to aggressively test the performance of electrodes printed directly on textiles, something the researchers say has not been done before. The textile of choice—elastic waistbands of underwear— highlights one potential application of the "hospital-on-a-chip" systems the electrodes will be part of: "smart underwear."



Chemical-sensing electrodes printed directly on the inside elastic waistband of underwear. Photo credit: UC San Diego/Daniel Kane.

The "smart" in "smart underwear" refers to the fact that the printed sensors will be incorporated into logic-based biocomputing systems that will monitor biomarkers found in human sweat and tears, make autonomous diagnoses and administer drugs. The smart system will automatically trigger the release of drugs held in reservoirs, in order to begin treatment before help arrives. All sensors, power, electronics and logic systems will be embedded in the clothing—such as the elastic waistband of underwear.

"The elastic waistband of common underwear has been selected as model clothing owing to its tight contact and direct exposure with the skin, and hence for its potential for direct sweat monitoring," wrote the authors of the Analyst paper.

Reflecting on the considerable interest the research on sensors embedded onto underwear has received, team leader Joseph Wang said "…putting the electrodes on the underwear, we didn't plan to make it so sexy. Our approach is scientific. The waistband of the underwear gives you the best contact with the skin where you expect to get a good sampling of the sweat. We just want the ones and zeros. The digital pattern of ones and zeros will reveal the type of injury and automatically trigger the proper treatment."

For example, if an injured soldier were to enter a state of shock, enzymes on the electrode would sense rising levels of the biomarkers lactate, glucose and norepinephrine. In turn, the concentrations of products generated by the enzymes would change. This will cause the built-in logic structure to output a signal that points to shock and, as a result, trigger a pre-determined treatment response.

"This is biocomputing in action," said Wang.

Read the entire release. (*www.jacobsschool.ucsd.edu/news/news_releases/release.sfe?id=958*)

iGo Green Laptop Travel Charger: One Less Vampire in the House

A study conducted by the Lawrence Berkeley National Laboratory discovered that so-called "electricity vampires—devices that provide constant power to electronic devices like cell phones, clocks, DVD players and laptop chargers whether they need it or not—account for approximately one-tenth of total residential electricity consumption in America. That's more than three billion dollars a year in wasted juice.

iGo's Green Laptop Charger (*www.igo.com/Green/Laptop-Travel-Charger-iGo-Greenr/invt/ps001330004*) (iGo PS00133-0001, $129.99 list) goes a long way toward exorcising these power suckers because it uses less than 15 percent of the standby power of standard chargers thanks to a clever automatic shut-off and recovery system that automatically reduces power when a device doesn't need it. That means you no longer need to unplug the charger to avoid wasting power—or feel guilty because you're starting to get unpleasant looks at your monthly Sierra Club

meeting.

The iGo Green is also a versatile device. You can charge almost any laptop whether you're at home, in the car, or on a plane. It works worldwide, so there's no need to fool around with voltage converters. Another useful feature: a built-in USB port so you can power many modern mobile phones and other devices.

Quick specs:

Dimensions: 6.7 x 2.77 x 0.64 in (170.18 x 70.36 x 16.26 mm)
Weight: 15.52 oz (439.98 g)
Input power: 100-240 VAC; 50/60 Hz
Output power: 90W

Package Contents:

iGo Laptop Charger
Laptop Input Cord
AC Input Cable
DC Input Cable
USB Charging Cable
User Guide

The iGo Green is an idea whose time has come. Hopefully we'll see this type of device become the rule rather than the exception.

Your Vest Friend When Traveling

When you prepare to travel, do you suffer from TMS—too much stuff? If so, SCOTTEVEST might have just the solution for you in its gadget-lovers' garments called Travel Vest for men (*www.scottevest.com/v3_store/New_Travel_Vest.shtml*) and Travel Vest for women (*www.scottevest.com/v3_store/New_Travel_Vest_Women.shtml*).

SCOTTEVEST is a TEC company rather than a tech company. TEC is technology-enabled clothing that "conceals a patented conduit system inside garments, known as the Personal Area Network (PAN), allowing you to wire your headphones from your MP3 player and/or cell phone, without the mess of wires" (more on this in a minute). As such, TEC products afford at least two potential benefits. First, they could minimize time spent fussing with earphone cables while commuting via mass transit, biking, jogging, or hiking. Second, TEC products exemplify SCOTTEVEST's philosophy that travelers should wear all of their devices and accouterments within their clothing rather than stowing them in fanny packs or backpacks. Upon approaching an airport's security checkpoint, you simply remove your TEC product (*www.scottevest.com/presskit/pressreleases/press_release_tsa_04_2010.pdf*) and pass it through the detector rather than scanning your stuff individually or paying an extra baggage fee. Cool!

One of SCOTTEVEST's many TEC products is the Travel Vest. It has a Teflon-coated outer shell (65 percent cotton and 35 percent nylon) and an inner lining (100 percent polyester) that are

machine washable (cold with like-colored garments; no bleach) and dry-able (tumble at low heat). The Travel Vest comes in three colors (Black Lava, Desert Sand shown in Figure 1, and Red Rock) and multiple sizes (S to XXXL for men; XS to XXL for women). Although its $100 price tag might seem high, this product is very useful (as we'll see momentarily) and backed by a customer-friendly two year guarantee (*www.scottevest.com/company/popups/our-guarantee-returns-exchanges.shtml*).

Figure 1. Travel Vests for men (left) and for women (right) are highly practical and versatile replacements for a gizmo-toting fanny pack, backpack, or luggage. They come in three colors (Desert Sand is shown) and a wide range of sizes.

One of Travel Vest's key features, as mentioned before, is its Personal Area Network. Although this feature's name might conjure up notions of high tech, it is instead a low-tech but quite clever earphone cables manager. PAN consists of three fleece-covered Velcro straps that comprise the vest collar's interior, two elastic loops, a snap-loop, and two firm plastic conduits built into the Travel Vest's liner about two inches below the collar on each side (see Figure 2). Just pass your earphones' cables through the loops and plastic conduits, secure the Velcro straps, and voilà—say goodbye to tangled cables!

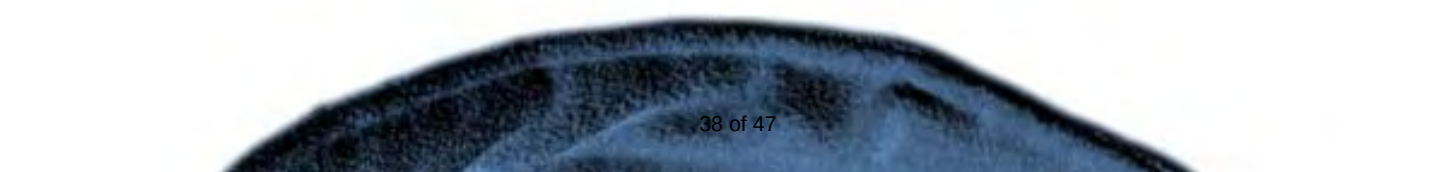


Figure 2. X-ray view of the Personal Area Network in action. Earphones' cables are restrained by three Velcro straps, two elastic loops, and a snap-loop on the vest collar's interior, plus a plastic conduit below the collar on each side.

Another key feature of Travel Vests is the 22 (yes, 22) pockets, designed to conceal their contents rather than protruding. These pockets come in a wide variety of sizes to accommodate various gadgets—music players, cell phones, battery rechargers or power bricks, point-and-shoot digicams, digital media cards, earphones, USB pen drives, netbooks and eBook readers. In addition, one of the Travel Vest's pockets is big enough for an iPad and two others are specially designed for touch-interface devices (see Figure 3).

Figure 3. Travel Vest comes with one interior pocket large enough to hold an iPad without bulging on the outside (left); two other pockets have a see-through material for gadgets with a touch interface (right).

But wait, there's more! Travel Vest's other pockets can hold non-tech items such as travel documents (tickets, passport, etc.), driver's license and business cards, dinero, pens, a water bottle, keychain, eyeglasses, newspaper or magazine, human hands, and so on. An extensive list of items that fit in Travel Vest pockets is available on SCOTTEVEST's Web site (*www.scottevest.com/v3_store/New_Travel_Vest.shtml*). Although Travel Vest's name implies that this garment is intended for use when traveling, my tests confirm that it can be worn under almost any other circumstance. I've worn the Travel Vest while biking, commuting on buses and trolleys, walking, working at the office, and doing chores at home (good thing it's machine washable!). This product is warm, comfortable and convenient without being intrusive or appearing unprofessional.

In case you're thinking that utility vests are a dime a dozen, Travel Vest is distinguished by its amenities and attention to details. For example, each interior pocket has an icon label and a laminated informational card (2 x 3.5 inches) indicating the pocket's intended function. The eyeglasses' pocket contains a cloth for cleaning smudged lenses and an alligator clip on a cord to keep the cloth from escaping. One of the two hand-warmer pockets includes an elastic strap

for holding a water bottle upright within the pocket, and this pocket also includes a coiled cord with a lobster claw at one end for holding a keychain. The interior pockets with small dimensions are closed with Velcro rather than a zipper, and the Velcro comes with a little cloth tab to make opening the Velcro a bit easier. Lastly, one of several information cards has a disclaimer that the garment contains magnets that potentially could affect magnetic media, security scanners, or pacemakers. The card also claims that SCOTTEVEST has received "no complaints" about "interference" due to the magnets. However, this warning might be moot; the Travel Vest I tested did not have any magnets that I could find.

The only potentially serious downside to the Travel Vest is its price. Less expensive competitors exist, but you get what you pay for, and Travel Vest clearly is a quality product backed by the aforementioned generous guarantee. Less serious quibbles have to do with the pockets for touch devices. If you put an iPad in its appropriate pocket and zip the Travel Vest, forget about sitting or riding a bike; the iPad and your thigh will be at odds with each other. The workaround is to leave the Travel Vest unzipped to prevent silicone and flesh collisions (though at the risk that the iPad's weight will be unsupported and/or potentially stretch part of the Travel Vest's material). If you put a smartphone or touch-enabled music player in its see-through pocket, navigating between playlists or typing a phone number can be awkward and prone to mistakes. Workarounds are to use earphones equipped with remote controls, or remove the device from this pocket, do your business, and then put the device back in the pocket.

All told, the Travel Vest is a practical and useful low-tech TEC product that can simplify life with your high-tech mobile devices. Instead of sweating the price, think of it as an investment.

reviewed by Barry Fass-Holmes

In addition to being an editor and columnist for *ComputorEdge* and *ComputerScene* Magazines, where he has written hundreds of feature articles and cover stories over the past decade, Charles Carr has also penned well over 1,000 non-tech newspaper and magazine articles and columns for various publications, including two widely-read columns each week for San Diego's *North County Times* newspaper.

Carr has covered such diverse topics as pesticide use in area schools, invasive background checks for county volunteers, asthma awareness, the debate over standards-based grading, potential vulnerabilities in electronic voting machines, and Southern California's devastating 2003 and 2007 wildfires. He has also written many humorous pieces.

Carr has also edited dozens of stories and articles written by others which have appeared in major publications and web sites across the country.

He has been a contributor and technical advisor to *L.A. and San Diego Parent* magazines and receives dozens of requests a year to appear on Southern California television and radio stations to talk about important events in the tech world.

Carr has judged many writing competitions including San Diego Press Club and Time-Warner Communications contests and was sole judge for the national NAPPA Tech Toys awards for five years (which his kids really appreciated). He was recently a judge for the national "Poetry Out

Loud" competition.

He has won many writing accolades, including Press Club awards for Best Column Writing, Consumer Writing and Best Arts and Entertainment, and has repeatedly taken top honors in San Diego Songwriter's Guild competitions for his original musical compositions.

Carr will soon publish his first book, *What a World*, a collection of his best writings.

Learn more at *www.charlescarr.com*.

Return to Table of Contents

EdgeWord: A Note from the Publisher

“Make technology work to protect yourself from ID theft.” by Jack Dunning

In spite of all the new techniques for securing our information, we will always be susceptible to the actions of nefarious people. Technology is often our best defense against the technology being used against us.

In the old days credit cards were run through a machine to make a carbon copy impression on a charge slip. Every time the card was used, there was a dangerous piece of paper (with copies) produced bearing both the credit card number and a signature. There was even a period of time when it was common for merchants to ask for a telephone number to write on the charge slip. (I would often say, "I don't know why you ask for my number—you never call!") If that system were still in place, the credit card theft problem would be much worse.

Today, the paper credit card receipts bear only the last few digits of the number. If you still receive your statements in the mail, they no longer contain the complete account number. If someone needs to identify you over the phone before giving out information about one of your accounts, they ask for only the last four digits of your Social Security number. When logging on over the Web, the user ID and password are no longer enough. We also must remember the answers to our secret questions. "What was your mother's favorite ice cream?" There are many more protections built into today's system of financial transactions.

In spite of all the new techniques for securing our information, we will always be susceptible to the actions of nefarious people. There will be people in a position (whether a restaurant worker or an employee of a financial institution) to get their hands on our numbers. There is no absolute protection against unsavory types of people. Ultimately, it is up to us to protect ourselves.

Technology is often our best defense against the technology being used against us. Credit card companies have developed algorithms that analyze credit card use patterns. If something falls out the normal buying pattern for a credit card holder, the account is referred to an administrator who will follow up. There have been times when I've been queried about a particular purchase just to confirm that I was the person who actually made the transaction. Once a company identified thousands of dollars in purchases on a card that I rarely ever used. They called to let me know that I would not be responsible for the charges. Yet, even the best systems will not detect all fraud.

One of the best ways to protect yourself is to make the technology work for you. Today you can use the Web to access any financial account you may own. If you log into your accounts for your credit cards, you can immediately see any new transactions. In the past, to detect any fraud, unless you called the company, you had to wait until you received your monthly statement. If you regularly check, there is now much less time for the thief to run up a bill. However, if you own a number of accounts, logging into all of them can become quite tedious. There is a better way.

This year I started using Intuit's Quicken to track my finances (or lack of finances). One of its best features is the ability to create a vault of passwords—which incidentally has a password of its

own for access. Once the vault is set up with the account numbers, login Web sites and passwords, all of the data can be downloaded and updated at any time without visiting the individual Web sites. This automates the process of checking the activity and downloading new transactions on all credit cards and will quickly tell me if there is any unusual activity. It is now easy to check everything at least once a day without any real extra effort.

My guess is that most money-management software now includes this batch downloading capability. I just happen to use Quicken. If I had to personally log in to each Web site when checking activity, I'm sure that I wouldn't do it every day—I never did before. But now I'm just a little more protected because I check regularly. All I have to do is look at the downloaded information.

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

"Virtual Machines," "Outlook Express Error Message," "Cox Spam," "Keep Up the Good Work"

Virtual Machines

[Regarding Pete Choppin's June 18 article, "Virtual Machines: What They Are and What They Can Do":]

This is directed toward last week's virtual machine article and Oracle's VirtualBox. I have an issue with downloading and streaming video that I will take up in a separate e-mail (it took me almost an hour to download). Anyway, I finally got it to run and loaded XP (I didn't check the disc and loaded plain-Jane XP from 2002. What a dog). When I got XP to run I discovered that I couldn't access any of the optical drives on my host computer (I'm running Win 7 Home Pro in a Gateway 4300, with 8 gigs RAM and a 1 terabyte disk, 2.4GHz AND quad core processor and ATI Radeon HD 4600 Series graphics processor). I have an internal DVD multi R*bckslsh*W and external USB Optiplex double-layer DVD writer. Also, I cannot access either of the two share folders that I set up in the virtual machine settings. I did get Internet access, but can't access the host machine's hard drive. Any help you can give me on this?

I have another question: Are you really emulating an XP machine when you create a virtual machine in a computer like mine?

Yours,

-Buck, El Cajon, CA

Buck,

I have looked into some of your issues (on Google and the VirtualBox forums) and have found some vague references to a few of the problems you have, but nothing concrete. There does seem to be some limitations with some USB devices.

You should also consider installing the Guest Additions, which provide more functionality to VirtualBox. I doubt this will resolve all your issues, but it will make life a little easier for you.

Networking on VirtualBox can be a little tricky. VirtualBox offers a few different types of network setups (NAT, Host Only, Bridged), and depending on which you chose will determine how your guest OS will function on the network.

VirtualBox also has a strong community of users. I would check out their forums. There are tons of users willing to help you. Also, I don't know if you have ever used IRC, but VirtualBox does

host an IRC chat. These are live users on text chat that can help you find answers as well.

*VirtualBox Community (*www.virtualbox.org/wiki/Community*)*

-Pete Choppin

Outlook Express Error Message

[Regarding the July 2 Digital Dave column:]

Dave, you are a genius! And that's why I have been a subscriber for so many years. I did what you suggested, and behold, it worked. Thank you so much. Keep up the good work.

-Gabby DeDonato, San Clemente, CA

AT&T does indeed use SSL for its e-mail account. My guess is that they changed their POP3 and/or SMTP port number again. Google "AT&T POP3" to see which port it is using now. Hope this is helpful.

-Edward, San Diego

Cox Spam

[Regarding the June 25 Spam of the Week: Amazon.com column:]

I got this e-mail June 14 and thought I would share it with you. It is directed to Cox cable users and does look official except for the grammar and formatting. It doesn't have any links in it, but just to be safe I have copied the text of it and pasted it into this e-mail; this is how it was formatted when I received it.

PS: The actual, "from" address showed up as "louandori @ Cox .net" (I put in the spaces so it would not be turned into a link by Incredimail.)

This message is from (COX COMMUNICATIONS) kindly send your Login Information

Because we noticed your account is being accessed from three different
Location

Your Username and Password will be needed to stop this act, once
This is done,
Your mail will begin to work as normal

Failure to do this within 24 hours will result to shutting down of your
Account, Login information: USERNAME.....PASSWORD.....DATE OF BIRTH
Should be
Sent as soon as you receive this mail.

Thank You for using COX.

-Buck, El Cajon, CA

Keep Up the Good Work

[Regarding the July 2 Windows Media Programs column:]

Jack,

I think that you have hit upon a topic of interest to a lot of us. Your Windows Tips & Tricks column has been extremely interesting; however, your last columns have seemed to cry for a new topic. I have an HDTV-enabled 24-inch monitor driven by a desktop with integrated tuner and gaming video card all hooked into Cox cable. The setup I have is an absolute "kludge," as nothing works correctly with anything else. I've spent hours and hours looking for solutions with very little success. Keep up the good work.

-Don Pillar

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*.

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