



“As a business owner, I know you don’t have time to waste on technical and operational issues. That’s where we *shine!* Call us and put an end to your IT problems finally and forever!”

- Matt Weaver, Echo Systems

August, 2010  
Bridgeville, PA

### Inside This Issue...

Do you use Facebook or Twitter, do you use employees? You **MUST** read this now!.....Page 2

A NEW Security Threat You Must Know About And Address Immediately.....Page 4

New Screen Capture Software You’ll Quickly Fall In LOVE With.....Page 5

Can Your Company Be Sued For Employees Who Use Their Cell Phones While Driving?.....Page 5

Are Extended Warranties Worth The Money? 5 Tips You Should Know Before You Buy.....Page 6

Techie Terms Made Simple: What Is Cloud-Based Computing?.....Page 6

*“Insider Tips To Make Your Business Run Faster, Easier, And More Profitably”*

## Echo Systems Prints Its First Client Newsletter!

It’s been a long time coming, but you’re holding the first issue of Echo Systems “Tech Times.” Tech Times will be a monthly newsletter (usually arriving around the 15th of the month) containing news about industry trends, tips and hints on software, and occasionally something just plain silly.

It’s my intention to use this newsletter to share information about upcoming technologies which will change the small and medium business space, as well as threats and situations I’ve come across with technology that could have been prevented had folks been more informed.

This newsletter is also sent out in an electronic PDF format, if you know anyone who might be interested in receiving this through email, please contact [info@echosystems.us](mailto:info@echosystems.us) to have them added to the mailing list!

I hope you enjoy these newsletters, I’m always open to any suggestions or criticism, please don’t hesitate to contact me ([info@echosystems.us](mailto:info@echosystems.us), or **724-941-9130**) for anything.

-Matt Weaver  
Echo Systems

**Watch It...**

Watch your thoughts;  
they become words.

Watch your words; they  
become actions.

Watch your actions;  
they become habits.

Watch your habits; they  
become character.

Watch your character; it  
becomes your destiny.

*~Frank Outlaw, founder  
of Bi-Lo Supermarkets  
in South Carolina*

**Just For Giggles...**

"Say you want to huff and puff and blow a house in...there's an app for that."

## Attention Facebook & Twitter Users: Hackers Are Now Using Your Friends Accounts To Transmit Viruses

**“Hey, I have this hilarious video of you dancing. Your face is so red. You should check it out!”** If you've received a message like that through a Facebook or MySpace friend, you may have been exposed to the "Koobface" virus. Here's what's going on...

Hackers have now made a new cozy home for themselves on social media sites such as Facebook and Twitter. Disguised as one of your friends, they'll send you a direct message with a video link attached. If you click on the link, you're prompted to update your Flash player to see the video, and therein lies the virus, cloaked in a "flash\_player.exe" file. Once installed, this worm transforms your computer into a Zombie machine as part of a botnet (a network of computers that are controlled and used by the originator of the worm for unscrupulous purposes).

### Are You Really At Risk?

Unless you are aware of these scams, it is very easy to become infected. Some of the direct messages and tweets have titles that are very deceptive. Some of the more common messages will say, "Here's the video I mentioned...", or "LOL," or "My friend caught you on hidden cam," or "My home video :)" These messages are followed by a link directing you to a page to watch the video. These seemingly harmless messages can quickly infect your entire office network, allowing hackers a free pass in. In addition, they can block you from accessing important security updates, making your network even more susceptible to hacker attacks. In some cases, they use their free access to your computer to steal bank account information, credit card numbers, social security numbers and other confidential data.

**(724) 941 - 9130**

Get More Free Tips, Tools, and Services At My Web Site: [www.EchoSystems.US](http://www.EchoSystems.US)

## That's one fancy pen!

First there were smart phones. Now, there are smart *pens*.

The new smart pen by Livescribe (called the "Pulse") electronically records all the words you write and simultaneously records the audio as well. Here's how it works...

While you're taking notes on its special dot matrix paper, the Pulse's microphone records the presentation or speech going on in the room. If you want to review a section of your notes, simply hold the pen over that area of the paper and the smart pen will replay the section of the audio recording that coincides with those notes.

The pens cost \$200. The paper can be printed for free from a Color LaserJet Printer that is Adobe PostScript compatible and can print at 600 dpi or higher. You can also purchase the dot paper notebooks for around \$14. Now there are no excuses for missing any part of a presentation!

## How To Protect Yourself

Awareness is the first step to protecting yourself. Make a copy of this newsletter and hand it out to all your co-workers and your friends and family so they don't get infected or infect you. Next, follow these three simple steps:

- 1) Frequently Change Your Password And Don't Use Easy To Guess Combinations.** I know, it's a pain in the neck to change your password frequently, especially when you have dozens to keep track of. But this really is one of the best ways to avoid compromising your account on social media sites. Additionally, don't use simple passwords like "password" or "123abc." Include lower case and capital letters, as well as numbers. If a hacker is trying to crack your password and you never change it (or if it's super easy to guess), you make your account a prime target.
- 2) Avoid Downloads.** Avoid downloading anything from messages on Twitter or Facebook, even if the message is from someone you know. As a general rule, never download any file if you are not 100% certain it is secure and virus free.
- 3) Get A Beefy Firewall.** If you or your employees are using any social media sites for personal or business connections, a strong firewall will protect you from getting infected. That way, even if you or your staff inadvertently opens a dangerous message from one of these sites, your firewall can prevent it from bringing your whole network to a grinding halt.

**If you'd like more information on the importance of securing your network against social media threats, please e-mail us at [info@echosystems.us](mailto:info@echosystems.us) or call us at 724-941-9130**

## **Shocking New CBS News Report Reveals Why Your Office Copy Machine Is Actually A Security Time Bomb**

This just in: According to a recent CBS news report, copy and multi-function machines in offices contain a huge, unknown security risk that all businesses must address immediately or face the legal, financial, and PR repercussions of a security breach.

### **A Surprising Fact About Your Office Copier**

Nearly every printer, copier and multi-function machine manufactured after 2002 contains a hard drive that stores the images of every document you've ever copied, faxed, or scanned. These document images stay on that machine's hard drive forever and can quickly and easily be reproduced with a little know-how. Surprisingly, this little fact has not received any press – until now.

### **A CBS Undercover Investigation**

In April of this year, a reporter went undercover to a New Jersey copier warehouse that had over 6,000 used copy machines in stock for resale. This investigation reveals a shocking fact – it's incredibly easy for a person to retrieve and reproduce every single document ever scanned, copied, or faxed through the machines available for resale.

As part of the investigation, the CBS reporter pulled 4 random machines that were available for sale and purchased them for approximately \$300 each. These machines were immediately loaded onto a truck and delivered within 2 hours to this reporter's office. Using a free application available online, he was able to access the hard drive of each machine and reproduce the documents within 30 minutes. What he uncovered was unbelievable.

### **Disturbing Facts Revealed By The Investigation**

They discovered that one of the machines was formerly owned by the City of Buffalo, New York, Sex Crimes Division. In no time at all they were able to access over 249,000 documents that passed through that machine, including lists of sex offenders and crime data. Another machine from the Buffalo PD Narcotics Division contained a list of drug raid targets. The third machine was from a construction company. It contained blueprints of buildings, over \$40,000 in check copies, as well as pages of paystubs, names, and the social security numbers of employees.

But the fourth machine was the most disturbing. It was previously owned by a New York health insurance firm and contained over 300 pages of detailed medical records including drug prescriptions, blood tests, and even a cancer diagnosis – all which blatantly violate the new HIPAA laws.

### **Know What Your Responsibility Is**

Before you trade in, resell or dispose of any office copier, scanner or multifunction machine you **MUST** make sure the hard drive is wiped clean of all information as you would any computer in your office. Failure to do so could result in damaging security breaches and identity theft for your company, staff, and customers. This goes **DOUBLE** if you use your office machines to scan, fax, or copy social security numbers, credit cards, or medical records of any kind.

As always, we are here to assist you with all things digital. If you are getting ready to dispose of or trade in a copier, scanner, fax, or multi-function machine, give us a call. We can make sure your data is forever erased and inaccessible to criminals looking for an easy hit.

## Shiny New Gadget of the Month



### *Snagit By TechSmith*

This month's pick is not really a gadget. It's a cool, inexpensive software program you'll easily get addicted to. Snagit is easy to use screen capture software that allows you to copy, edit, share and organize images captured off of your computer screen. The more you use Snagit, the more ways you'll find to use it.

For example, if you are working with a designer or programmer to develop a web application or web site, Snagit will allow you to capture a screen shot of the web page and add comments, cut and paste sections, add instructions, edit the design, and much more, making your communication much more precise and clear.

Creating a user guide or instruction manual? You'll love Snagit because you can capture segments of a computer screen and add comments and instructions right over the area (or document) you are explaining, making even the most complicated processes and software easy to follow.

Best of all, you can store these images in various image files (jpeg, png, gif, etc.) and cut and paste them into an e-mail, Word document, web site, etc. Snagit costs \$49.95 for a single user license and can be purchased at [www.techsmith.com](http://www.techsmith.com). If you want to try before you buy, you can download a 30-day free trial at the above web site as well.

## Business Owner Beware: You Can Now Be Held Liable For Accidents Caused By Employees Who Are Talking On Their Cell Phones Or Texting While Driving



Over the past several years, states have been instituting laws to limit the use of cell phones while driving – so how does this affect companies who have employees using company vehicles? Quite a bit, actually.

Several lawsuits have cropped up in which a company was sued for an employee causing an accident while talking on a cell phone. In Virginia, an attorney driving home from work ran over a teenage girl, killing her. The family of the girl filed a \$30 million lawsuit against the employer because the attorney was talking to a client when the incident happened.

In the state of Arkansas, a jury found a lumber company liable after one of their employees struck another car, gravely injuring the passenger. At the time of the accident the employee driving the vehicle was using a cell phone for a sales call. That particular case ended up being settled for \$16 million.

Many states have defined hands-free laws and produced legislation that bans cell-phone use completely. Although employer responsibility isn't specifically defined in the cell phone legislation, there have been an increasing number of lawsuits relating to employer responsibility regarding mobile cell-phone use for employees. Hands-free laws have done little to protect employers from liability, and as the trend of cell-phone legislation increases, employers should be prepared to address their mobile workforce and advise them of the cellular phone laws that are in effect in your state or locality.

We recommend you talk to your attorney about implementing a mobile phone and vehicle use policy that all employees must sign. While this may not completely remove your risk of being held responsible for accidents or injuries caused by employees driving a company-owned vehicle, it does show some forethought and responsibility on your behalf.

## Good News For Early Adopters...

It's good news for business travelers and vacationers alike.

The Transportation Security Administration says the iPad won't have to be removed from carry-on baggage at security checkpoints. It's just half-an-inch thick and has no parts that can block images when the machines go through the screening machine.

Electronics that are smaller than the standard laptop, such as the Kindle, Sony Reader, and small notebook computers, can also stay in the bag.

But it's not an actual rule. Screeners still have the discretion to ask that the devices be removed in order to further inspect them or the cases they are in.

The TSA recommends checkpoint-friendly bags that have a separate laptop flap that can be unfolded flat on the machine belt.

## Are Extended Warranties Worth The Money?

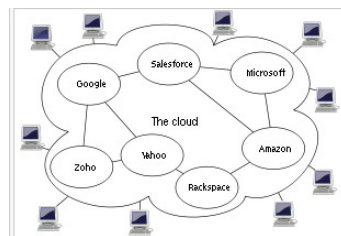
Seems like you can't purchase any electronic device without being offered an extended warranty—but is it a good investment? According to a recent poll of over 2,000 readers of PC World magazine, 63% said they always go for the extended warranty plan; and of those who had to use it, 80% were satisfied with the service. Does that mean they are a good investment?

In our opinion, extended warranties are not necessary since most bugs will reveal themselves within the first 90 days of purchasing a technical gadget, which is well within the normal warranty of the product. But if you feel better buying an extended warranty, here are 5 tips to follow:

1. Read the terms before you buy: You don't have to read the warranty in the checkout line—take it home. You can usually buy it later.
2. Beware shipping charges: If the product needs to be sent in for service, you could get stuck with the tab.
3. Look for accidental damage coverage: Most policies do not cover products that are damaged from falls or spilled coffee. If that option is available, you might have to pay more for it (a good idea, particularly for mobile devices that get abused).
4. Look for extras: Many extended warranties cover replaceable items, such as bulbs in projectors which are expensive and can wear out.
5. Check for the product's reliability online first. If you are buying a quality product, an extended warranty might not be necessary. Obviously doing a little research and spending a bit more on a better built product will save you a lot of time and aggravation in the long run anyway. You can find some good information in PC World's annual Reliability and Service survey and Consumer Reports' reliability ratings.

## Techie Terms Made Simple: What Is Cloud Computing?

Cloud computing is simply a term used to describe internet-based applications that are stored and accessed via a web browser instead of a server or computer at your location. Over the last couple of years there has been a HUGE movement towards companies using “cloud-based” applications because lost data is more easily recovered and remote workers can conveniently access information. As a result, costs for hardware and support are drastically lowered.



One “cloud” application we encourage our clients to consider is Hosted Exchange. Not only does this give you a tremendous amount of flexibility in accessing your e-mail, but it also lowers the costs of hardware, software, installation, and support **DRASTICALLY**.

While there are still some fears around hosting critical apps and data offsite, those fears will become a thing of the past as business owners see the bottom-line cost savings of cloud-based computing.