



# BUSINESS TECHNOLOGY QUARTERLY

Brought to you by **The Technology Group, LLC**

(860) 524-4400 [www.TheTechnologyGroup.com](http://www.TheTechnologyGroup.com)

## Malware? In MY Computer?

By: Ian Cranston

Many of us are familiar with malware, the sneaky, malicious software that causes computers to slow down, crash, make pop-ups, and act strangely. But where does it come from and how do we stop it?

The most common ways that malware infects a PC are either by clicking a link or downloading a file from an email crafted to spread the malware, or by visiting a website designed to spread the virus. You can get a virus simply by going to an infected website without clicking or downloading or agreeing to anything.

*(Continued on page 5)*

## Are You Eligible for a Free Windows 7® Upgrade?

By: David Modzelewski

Usually, when Microsoft has an upcoming new operating system release, many PC manufacturers (Dell, HP, etc) will offer a free upgrade on the new system, even if it hasn't been released yet. This is certainly the case with Windows 7. If you or your company has recently

*(Continued on page 6)*

### No Contracts. Just Solutions.

**Don't pay for technology support hours you don't use!**

Call for Details

**860.524.4400**

[www.TheTechnologyGroup.com](http://www.TheTechnologyGroup.com)

## Windows 7 Compatibility



By: Michael Brown

With the recent release and high praise of Windows 7, many are asking if it's time to upgrade. Although the end of support for Windows XP is still a long way off, with security and patches being released until April 8, 2014, it is a matter of great concern for many users and Microsoft has made great strides in preparing Windows 7 for compatibility.

In the case of upgrading the operating system on your current computer, while the system requirements to install Windows 7 are not terribly stringent, it does require:

- 1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
- 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
- 16 GB available hard disk space (32-bit) or 20 GB (64-bit)

*(Continued on page 6)*

## INSIDE

Viruses, Worms, Trojans...What's the difference?	pg. 2
Vulnerabilities in Encryption Technologies	pg. 2
Non-Profit Spotlight - Knox Parks Foundation, Inc.	pg. 3
For Non-Profits Only - Sage MIP Budget Versions	pg. 3
Security News	pg. 4
Breach Alert: Time to Take this Security Thing Seriously...	pg. 4
In-house News	pg. 6
Microsoft Exchange® 2010	pg. 8

## Viruses, Worms, Trojan Horses, Spyware, Adware, Malware – What's the Difference?

By: Ian Cranston

Each term has a specific definition, but they have been used so interchangeably over time that their meanings are ambiguous to everyone except technology grammar sticklers (i.e. nerds). Adding to the confusion is that many malware programs now blur the line and fall into multiple categories. For example, the wide-spread "Vundo" malware uses a Trojan horse attack to infiltrate a computer and then acts as adware. Keeping that in mind, here are some useful explanations.

A virus is a computer program that can copy itself and infect a computer. What makes a virus unique is that it can only spread when it is sent or transferred by network file share, e-mail, CD, USB stick or other medium, and then run (or inserted in the computer) by the user.

A worm is similar to a virus in that it can copy itself and infect a computer but a **worm** spreads itself by exploiting security vulnerabilities over a network without user intervention.

A Trojan horse is a program that appears to be desirable but does something undesirable. An example of a Trojan horse is "Smiley Central,"

which adds cartoon smile emoticons to email, but also installs a slew of spyware. Trojan horses do not copy themselves.

Spyware is malicious software that secretly gathers information such as e-mail addresses, passwords, web browsing habits, and other personal information and sends it over the internet.

**Adware** is malicious software that displays advertisements, usually as pop-ups. Adware can also appear as software on the machine, often posing as anti-virus or anti-spyware software running a fake scan that detects critical items to goad the user into entering a credit card number to purchase the software.

**Malware** is short for malicious software. It is any software that is designed to infect or damage a PC and encompasses all of the above terms.

## Vulnerabilities in Encryption Technology

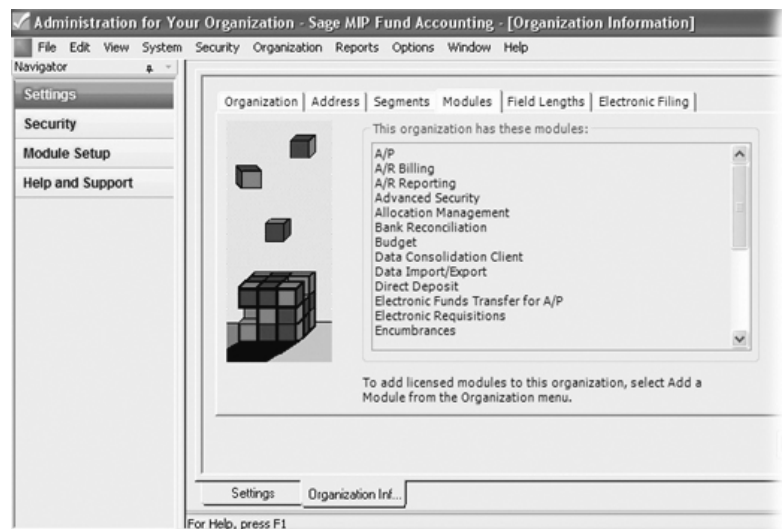
By: Gregory Rothausser, MCSA

Security on mobile devices such as laptops has been made better by the invention and widespread use of whole-disk encryption technologies like PGP, Bitlocker or TrueCrypt, but these encryption technologies can be vulnerable to certain kinds of exploits. Many mobile users have cached copies of their email or documents via Offline Files stored on their devices. Those documents and emails are vulnerable to theft and unauthorized access even when the laptop is encrypted. Three of the most widely known and dangerous encryption technology vulnerabilities are

(Continued on page 3)

## MIP Tips and Tricks

### Fund Accounting – Modules? What Modules!



Do you know what MIP modules your organization owns? Do you have modules you don't use? To determine this information go to Administration/Organization Information/Modules.

## Vulnerabilities

*(Continued from page 2)*

called “frozen boot,” “stoned boot,” and “evil maid.”

The Frozen Boot only works on a laptop device that is physically stolen while powered on or in suspend mode. In this locked state, researchers found that if memory chips are frozen using compressed air or other easy-to-obtain methods, the contents of memory will remain readable for 30-60 seconds after power loss. This gives a thief enough time to freeze the memory, attach a USB hard drive, and reboot the machine. The attacker's bootable device would then read the contents of the laptop's memory and dump it to a file on the USB drive. Once the file has been dumped, the encryption key can be retrieved and contents of the hard drive read at the hacker's leisure.

The Stoned Boot attack - a “rootkit Trojan horse virus,” - means the attacker does not need physical access to your machine. They need only find a way to infect your PC - whether via an email attachment or another method. Once your PC is infected with the virus, it copies itself to a part of your hard drive called the “Master Boot Record” - a part of your hard drive that is not encrypted - and runs before anything else. The virus can hide itself completely from Windows and from the user. Once you are booted up into Windows with this rootkit running, it can spy on the contents of your hard

*(Continued on page 5)*

## Non-Profit Spotlight Knox Parks Foundation, Inc.

For more than 40 years, Knox Parks Foundation works in partnership with residents, businesses and government to build stronger, greener and more beautiful communities in Greater Hartford.

Knox Parks Foundation's major programs include the **Green Crew** that trains out-of-school youth in landscaping and gardening; the **Green Team** comprised of volunteers who come together to work on clean up, beautification, planting and graffiti removal projects; **Community gardens** where more than 300 families grow vegetables and flowers in fourteen locations throughout Hartford; **Hartford Blooms** where individuals and corporations sponsor more than 400 flowering planters placed throughout the City; and **Trees for Hartford Neighborhoods** which helps reverse the trend of urban deforestation in Hartford.

Knox Parks Foundation accepts donations but other **nonprofits** can easily help Knox Parks Foundation by hiring the Knox Parks Green Crew for their spring and summer landscaping.

**75 Laurel St.  
Hartford, CT 06106  
(860) 951-7694  
Contact: Ron Pitz, Executive Director**



## For Non-Profits Only Sage MIP Budget Versions

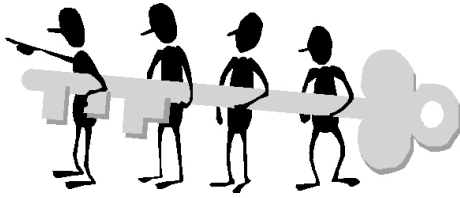
By: Linda Swanson

One of the great features of MIP's budget module is the ability to have more than two budgets for the same year. The budget module also allows you to have budget worksheets that can be “revisions” worksheet types. Here's the difference between **budget versions, budget worksheets, revisions worksheet**, and entering a budget without a worksheet.

**A budget worksheet** is a convenient way to speed up the budget entry process. You can choose the accounts and segments you wish to include in your budget, add posted comparison data, and automatically create the budget entries when transferred. When you create a budget worksheet, you choose the “budget version” you wish to use.

**A budget version** is a way to group selected worksheets or budget transactions together by the version ID. MIP has a version called “Original” and one called “Revised.” Within the budget module you can have as many as you need and you can name them as you wish. At the beginning of the budget process you probably will have an original budget version. But sometimes you need to change your budget and you want to keep your original budget intact as a Board-approved budget or

*(Continued on page 5)*



## SECURITY NEWS

(Courtesy of the Sans Institute unless otherwise noted)

### 2010 Date Recognition Problems

(January 5, 2010)

Smartphone users running Windows Mobile are getting text messages dated 2016. Symantec's Endpoint Protection manager is labeling signatures dated in the new year as being out-of-date; until the problem is addressed in an update, new malware signatures will be dated 12/31/2009 with increased revision numbers. Other vendors affected include Cisco, SpamAssassin.

### Full Body Scanners Used by TSA Present Privacy Concerns

(January 11, 2010)

According to documents obtained by the Electronic Privacy Information Center (EPIC), the full body scanners currently being used by the Transportation Security Administration (TSA) are capable of retaining and transmitting images.

The documents indicate that the Windows XP-based machines may be vulnerable to tampering. According to the Department of Homeland Security (DHS) website, the machines are delivered to

airports without the ability to store, print or transmit images. The ability to store and send images was reportedly enabled only during the machines' testing period. The scanners are not connected to each other, nor are they connected to the Internet. The machines are currently used in about 20 airports nationwide; the TSA plans to deploy them at all major airports.

### USB Flaws Prompt NIST Review of Cryptographic Module Certification Process

(January 8 & 11, 2010)

The National Institute of Standards and Technology (NIST) is investigating security flaws in several brands of USB drives that were thought to be secure. The vulnerability can reportedly be exploited to allow attackers to read data on drives protected by the 256-bit Advanced Encryption Standard. The vulnerabilities lie in the software that authorizes decryption.

NIST will be considering whether it should make changes to its validation process, as the USB drives in question all met the criteria. SanDisk, Verbatim and Kingston, the three companies that acknowledged the vulnerabilities in their devices, have issued fixes for the problem.

## Breach Alert: Time to Take this Security Thing Seriously...

By: Mark R. Torello, CFE, CISA

**Medical practice?** New HiTech provisions of HIPAA are no joke! And new state statutes apply as well.

**Non-Profit or family owned business?** Yes, new laws apply to you.

### Connecticut and Mass Have Tough New Laws that Apply to All Businesses

**For Massachusetts:** Every person who owns or licenses personal information about a resident of the Commonwealth shall be in full compliance with 201 CMR 17.00 **on or before March 1, 2010.** That law includes standards for the protection of personal information of residents of the Commonwealth.

The most recent regulation issued in August of 2009 makes clear that the rule adopts a risk-based approach to information security. A risk-based approach directs a business to establish a written security program that takes into account the business size, scope, amount of resources, nature and quantity of data collected or stored, and the need for security.

(Continued on page 7)

**Malware**

*(Continued from page 1)*

“Vundo,” the most prevalent and destructive malware right now (it also goes by many other names such as Sysprotect, Storage Protector, AntiSpyWareMaster, WinFixer, AntiVirus 2009 and similarly named programs that pop up and appear to do a scan for viruses), exploits a vulnerability in older versions of Java. The vulnerability in Java allows Vundo to transfer itself and run on your computer.

Even having anti-virus software won't necessarily protect your computer from Vundo.

Only the latest anti-virus software is able to

detect the worst types of malware before they install themselves.

Once installed, some strains of Vundo can be removed by running anti-malware tools but some dig so deeply that they are impossible to fully remove without formatting the hard drive and reinstalling Windows.

The best way to keep malware off of your computer is three-fold:

1. Keep your computer updated with patches to Windows, Internet Explorer, and Java;
2. Install the newest anti-virus software;
3. Be skeptical of unsolicited e-mail and stay away from suspicious websites.

**Vulnerabilities**

*(Continued from page 3)*

drive or your actions like password entry, etc.

Finally, the most recent vulnerability is called the “evil maid.” Unlike “frozen boot” it does not require the PC to be running, but it requires physical access to the PC – twice. First, so the attacker has access to the PC, and can boot from their own device such as a USB hard drive or CD.

This copies a program to the Master Boot Record which records the keystrokes for your encryption key. After the hacker has installed the evil maid program and waited until you have used your laptop, they can then retrieve the encryption key from the Master Boot Record and make a copy of the contents of your hard drive to read later. A laptop left in a hotel room during the day at a conference would be vulnerable to this attack. Clearly, just having encryption

technology on your company's mobile devices is not enough. Users should maintain physical possession of their equipment. Anti-virus applications need to be maintained and updated regularly.

**Worksheets**

*(Continued from page 3)*

comparison purposes. Within the Administration Module, create a revised budget version. As things change again, you can create a “revised 2” budget version, and so on. All of these budget versions can be brought into your financial reports so you can see where you started and where you are now with all your budget versions.

**A revision worksheet** contains existing **posted** budget items to a particular budget version and a column to enter budget adjustments. This will make an adjustment to your existing posted budget. You will no longer have the budget as originally entered to be used as a comparison.

If revisions are minimal, budget revisions can also be made by **entering budget transactions** without a worksheet. Navigate to Transaction>Enter Budget, assign a session ID, description, and choose the budget version you wish to revise. The remainder of the entry works the same way as a journal entry.

**“...having anti-virus software won't necessarily protect your computer...”**

## Windows 7 Upgrade

*(Continued from page 1)*

purchased a new desktop or laptop, that device may be eligible for a free upgrade to Windows 7.

Eligibility for the free upgrade option is usually determined by the date the device was purchased and can vary among manufacturers. We have listed some of the common manufacturers and their upgrade eligibility requirements.

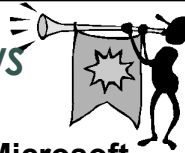
As always, there are additional "catches" and requirements stipulated by each manufacturer that may negate your system's upgrade eligibility.

Windows 7 is garnering many positive reviews and offers notable benefits when compared with previous versions. It is worth checking to see if your recently purchased system is eligible for a free upgrade.

### Free Windows 7 Upgrade Eligibility

Manufacturer	System must have been purchased between
Dell	June 26, 2009 and December 31, 2009
HP	June 26, 2009 and January 31, 2010
Lenovo	June 26, 2009 and January 31, 2010
Toshiba	June 26, 2009 and January 31, 2010
Acer	June 26, 2009 and January 31, 2010

## IN-HOUSE NEWS



### Engineer Earns Microsoft Certification; One Earns a Mate!

**O'Neil Carty**, in addition to holding a masters degree, has passed two of Microsoft's Certified Professional exams and is one exam away from the Microsoft Certified Systems Administrator (MCSA) certification.

**Ian Cranston** announced his engagement to Kelly King. Congratulations!

### The Children's Charity Ball

We sponsored one of our client's charity events, **The Bridge Family Center's The Children's Charity Ball**. The Bridge's 11th annual gala, will be held on January 23, 2010 at the Hartford Golf Club. It is the Bridge's signature fundraiser for its programs for children and families. More information can be found at [www.bridgefamilycenter.org](http://www.bridgefamilycenter.org).

### The Technology Group LLC would like to welcome the Following New Clients:

- South Central Area Agency on Aging
- Minore's Meats
- St. Vincent DePaul Place
- Lynn Community Health Center
- Community Resources for Children
- Simsbury Fire District

## Windows 7 Compatability

*(Continued from page 1)*

- DirectX 9 graphics device with WDDM 1.0 or higher driver

If you are sure your machine meets these requirements, Microsoft recommends you run the Windows 7 Upgrade Advisor. This tool is available for download from Microsoft.com and will scan your system for any hardware, driver, or software conflicts, and make recommendations on how best to proceed.

Another scenario to consider is that you are purchasing a new computer and want it preloaded with Windows 7. In this case you can be sure the computer's hardware will be compatible, but you may be left with questions regarding your favorite software or peripherals. To assist users in finding compatible products, Microsoft has a search tool with updated hardware and software information at on their site at Microsoft.com

You can search their database by product name or by using a convenient, categorized interface. Information is updated on the site as new solutions are found for existing issues and Microsoft continues testing products to ensure compatibility. Also located on the site are tutorials and solutions for installing and supporting applications written for older versions of Windows.



## New Laws

*(Continued from page 4)*

This new law is effective on March 1, 2010.

**For Connecticut:** A similar rule went into effect for October, 2008 requiring the duty to safeguard personal information. This law places new obligations on businesses that collect Social Security numbers ("SSNs") and other personal information, and levies substantial new penalties for privacy violations. The Act is not limited to businesses located in Connecticut or the personal information of Connecticut residents.

The Act requires any person who collects SSNs in the course of business to create a privacy policy that: (1) protects the confidentiality of SSNs; (2) prohibits the unlawful disclosure of SSNs; and (3) limits access to SSNs. Any intentional violation of the Act may be subject to a civil penalty of \$500 for each violation, up to \$500,000 for any single violation.

### If You Have a Medical Practice, there is Pressure from Congress to up Enforcement Efforts.

Congress has **mandated improved enforcement** of the HIPAA Security and Privacy Rule in the Health Information Technology for Economic and Clinical Health (HITECH) Act. The chart below shows results for Connecticut over several years.

## A Local Enforcement Case

A medical practice as close as Providence had to write a check for \$100,000 and implement a corrective action plan to the Department of Health and Human Services for backup tapes, optical disks, and laptops, containing unencrypted electronic protected health information that was left unattended and subsequently stolen. Investigations focused on the practice's failure to implement policies and procedures to safeguard this information.

The Corrective Action Plan required: revising its policies and procedures regarding physical and technical safeguards (e.g., encryption) governing off-site transport and storage of electronic media containing patient information, subject to HHS approval; training workforce members on the safeguards; conducting audits and site visits of facilities; and submitting compliance reports to HHS for a period of three years.

## Breach Notification Rule

Interim final breach notification regulations, issued in August 2009 and effective for September 23, 2009, implement

section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

## Breach Rule Requirements

If a breach affects 500 or more individuals, a covered entity must provide the Secretary with notice of the breach in no case later than 60 days from discovery. This notice must be submitted electronically via the breach notification form.

**Penalties:** There is a tiered penalty system in the regulation. Penalty maximums for tiers 1 through 4 are \$25,000, \$100,000, \$250,000, and \$1,500,000 respectively. The tier one falls in depends on culpability, looking at willful neglect, no corrective action plan, etc.

Luckily there are some good exemptions, one being encryption. If the protected health information is stolen or disseminated, but encrypted, you will not be in violation.

Your laptops and tablets are all encrypted, right? If not, give us a call and check this off your list for 2010. ■



**Microsoft Exchange 2010**

*By O'Neil Carty*

Microsoft's newest messaging server software solution features email, voicemail, calendar, contacts, tasks and support for mobile and Web-based access (Outlook Anywhere) to information and support for more data storage capacity.

It also enables new levels of reliability and performance with features that simplify your IT administration, helps protect your communications, and gives your users more flexibility by meeting their demands for greater mobility.

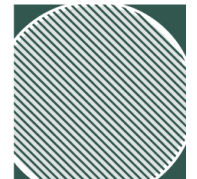
It can also safeguard your business with protection and compliance capabilities that help you manage risk.

**The Technology Group, LLC is proud to be allied with:**



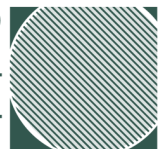
**WINTER 2009/2010 EDITION OF**

**BUSINESS TECHNOLOGY QUARTERLY**



147 Charter Oak Avenue  
Hartford, Connecticut  
06106-5100

The Technology Group, LLC



PR SRT STD  
U.S. POSTAGE  
PAID  
Hartford, CT  
Permit # 2639