



THE RHODENIZER REPORT

MAY 2008

www.rhodenizer.com

INSIDE THIS ISSUE:

WINDOWS VISTA ALREADY ON THE WAY OUT?	1
NCSA CALLS PC SURVEY RESULTS "ALARMING"	1
U. S. EMERGENCY ALERTS VIA TEXT MESSAGES SOON	2
QUESTIONS FROM THE INBOX	3
BLACKBERRY TIPS AND TRICKS	4
ABOUT RHODENIZER IT	4

WINDOWS VISTA ALREADY ON THE WAY OUT?

The next version of Windows is currently under development. While the official target date for release is still sometime in the year 2010, Bill Gates recently told the press that he expects to see a working version available for testing next year.

Simply named "Windows 7" at this point, it is hoped this new version will rescue Microsoft from the disappointment of Windows Vista. Much like Windows Me, another failed version of Windows, Vista seems destined to go down in history as another short-lived version of Windows that failed to meet expectations.

IT insiders have been complaining about Vista's slow performance and troubling compatibility issues since shortly after it's release in January of 2007.

In addition, many have ridiculed the main "security benefit" of Vista called UAC (User Access Control) which does nothing more than prompt the user incessantly with "Cancel" or "Allow" pop-up questions that the average person has no idea how to answer. Without the benefit of any additional information to consider, users eventually learn to answer "Allow" for every prompt if they hope to get any work done... thus, ne-



gating any real "benefit" as an early warning system at all.

To one with over 20 years of IT experience, this seems like a lawyer's idea to shield Microsoft in the event of a potential lawsuit. Having the user click "Allow" can be like signing a waiver every time you permit something new to (cont. P. 2)

THE TAKE-AWAY POINTS:

- **Windows 7 replacing Vista around 2010.**
- **Consumers' unsecured PC's aiding criminals.**
- **U. S. Government to send text message alerts to cell phones.**
- **Add memory to your Blackberry for \$10.**

NCSA CALLS PC SURVEY RESULTS "ALARMING"

The National Cyber Security Alliance (NCSA) reports that a majority of consumers don't understand "botnets" (networks of compromised PC's used to attack other computers), and don't believe their home PC's could affect homeland security.

At the RSA Conference in San Francisco, Ron Teixeira, executive director of the NCSA, said that "Botnets are an increasing threat to consumers and to homeland security. Consumers'

unsecured PC's play a major role in helping cybercriminals conduct cybercrimes - not only on the victim's PC, but also against others connected to the Internet." He went on to say that he considers it "alarming" that people don't know how to keep their computers secure.

According to their survey, 71% don't know what a "botnet" is; 59% don't believe their PC could affect homeland security; 47% don't believe it's possible

for their PC to be commandeered by hackers; 51% have not changed their password in over a year; and 48% do not know how to protect themselves from cybercriminals.

The results should come as no surprise since last October, a joint study conducted by the NCSA and McAfee found that almost half the consumers surveyed erroneously believed their PC's were adequately protected by antivirus software.

U. S. EMERGENCY ALERTS VIA TEXT MESSAGES SOON

Remember when, about once a week, the TV program was suddenly interrupted by an obnoxious tone? A black and white test pattern appeared on the screen. Then, *"This is a test of the Emergency Broadcast System. If this had been an actual emergency..."* Those of us that grew up in the 60's can still remember that annoying sound.

The EBS was established in 1963 by the FCC as a way for the President to address the nation quickly in the event of a national emergency. Controlled by the department of Civil Defense, it was designed to transmit across all AM, FM and TV broadcast stations.

The EBS was replaced in 1998 with the Emergency Alert System (EAS) which provides access to broadcast stations, cable systems, and satellite programmers for the

transmission of emergency alerts (and less obtrusive tests).

Digital codes developed by the National Weather Service can be used to activate devices in areas affected by an emergency. Even if you aren't listening, the EAS can signal specially equipped TVs, weather radios, scanners, etc., enabling them to activate (turn themselves on) to receive emergency alerts.

In 2006, Congress passed the **Warning Alert and Response Network Act**, which requires the FCC to upgrade the EAS so that all wireless carriers will have the ability to notify their subscribers of **emergency alerts via cell phone text messages**.

While the alert program has strong wireless industry support, operator participation is

still voluntary. Consumers will not be charged for any alert messages, and they may opt out at any time.

There will be three categories of text messages:

First Level: A national alert from the President, probably concerning a terrorist attack or natural disaster.

Second Level: Concerning "imminent threats" including hurricanes, tornadoes or nearby school shootings.

Third Level: Reserved for child abductions (Amber Alerts) and can be utilized by state or federal agencies.

Emergency messages will be delivered with a unique sound, or what the FCC calls a "vibration cadence." The cell phone text message emergency alert program is expected to launch by 2010.



WINDOWS VISTA ON THE WAY OUT? (CONT.)

(cont. from P. 1) run. If you allowed it, whatever happened is your fault.

Microsoft recently increased efforts to push Vista sales by dropping prices on the retail versions, and also by holding firm to the June 2008 deadline for ending retail sales of Windows XP.

However, faced with mounting opposition to Vista by the IT community, Microsoft is

also turning up the heat on developers to bring the next version of Windows to market as quickly as possible.

It has been my experience that difficulties are to be expected when making the transition to any new operating system. But, the gain should be worth the pain. I've yet to see anyone make a successful business case for upgrading to Vista from Windows XP Pro.

Perhaps the next version of Windows will give consumers a more compelling choice. Perhaps more application vendors will release versions of their products that run on Apple or Linux-based operating systems.

Until then, I continue to recommend refurbished XP Pro PC's instead of new Vista PC's for all small business owners looking for ways to save time and money. - C. R.

"... difficulties are to be expected when making the transition... But, the gain should be worth the pain."

QUESTIONS FROM THE INBOX

Q– “If my employee is caught doing something illegal on the Internet using one of our office computers, could I be in any kind of trouble?”

A– While I’m not an attorney and cannot give legal advice, I think any good attorney will tell you: “It depends”.

Did you know about it? Should you have known about it? Could this have been reasonably foreseen? Did you fail to do what any other reasonable person in your position would have done? These are all questions that you and your attorney should discuss.

From my experience in corporate IT, I can tell you that it was critical for us to have policies in place to protect the company in case something like this were to happen. We also had to enforce those policies consistently.

If there was a written policy against it, and you have been enforcing that policy consistently, and within reason, it would be very difficult for anyone to prove that you were complicit or negligent.

Therefore, I highly recommend that every business owner with one or more employees have an IT policy. It doesn’t have to be anything more complicated than just a list of things they are not allowed to do on company computers. Go over it in a group setting so there are

witnesses. Have each employee sign a brief statement to the effect that they understand the policies and agree to comply.

For more details, you should contact an attorney with experience in IT policies, or I can help you put together an IT policy manual. Then, have your attorney look it over.

Q– “What do I need to do to make sure our office computers are secure?”

A– There is actually no such thing as “secure” when it comes to computers. But, I understand what you mean. Making them reasonably secure is not difficult. Keeping them that way is.

An experienced IT pro can make your computer systems reasonably secure. But, whether or not they remain that way depends largely upon how you allow your people to use them. If you have no rules concerning allowable computer use, the actions of your employees could defeat any security improvements.

Start by implementing policies that define what is, and what is not permissible on company computers. Then, use IT to enforce those policies. We can employ various methods of blocking, scanning, and monitoring to ensure that your policies are

being followed, and that preventative measures are working as they should.

I offer a free initial consultation with no obligation. If you would like to learn more, I would be happy to go into more detail with you over a cup of coffee sometime.

Q– “In the last issue, you mentioned that the new AVG 8.0 Antivirus also has spyware and rootkit protection. What is a root kit?”

A– Root kits are the worst kind of virus. Unlike other malware that can be found and deleted, root kits alter your own system’s core files to perform new tasks. They can scan your system for commonly used antivirus programs and disable them. Then, setup a hidden base of operation for various attacks.

A large majority of antivirus products currently on the market cannot detect root kits, much less do anything to remove them.

The new AVG 8.0 is more than just antivirus software. It’s my choice for total system protection. You can download a free trial version from the “Cliff’s Picks” page of my website.

Send your questions to:
questions@rhodenizer.com



“A large majority of antivirus products currently on the market cannot detect root kits.”

OnGuard OnlineTM
YOUR SAFETY NET

Three simple words to help you be safer on the Internet

**STOP
THINK
CLICK**

Tips and Tools at OnGuardOnline.gov

BLACKBERRY TIPS AND TRICKS

Does your BlackBerry seem slower? Battery not lasting as long? This month, we look at some tips to lighten the load.

The two biggest battery hogs are the BlueTooth, and GPS modules. **Extend battery life by disabling one, or both, when you don't need them.** Google Maps also causes heavy battery drain. But, if it provides you with benefits that outweigh this cost, don't remove it yet. Just be aware of it. I'll watch for a new version that fixes this problem and report after I test it out.

Free up memory by moving pictures, ringtones, music,

and video to a microSD card (you can get a 2GB card for about \$10. It fits in a socket behind the battery). You can even set the camera to save pictures to it.

The BlackBerry keeps a log for troubleshooting purposes. **Keep your log file from growing too large** by holding down the "ALT" key and type "lglg" from the home screen. Once the log comes up, press the menu button (left of the ball) and select "clear". Then, close the log file.

See what programs are running in the background by holding the "ALT" key, then

press the back button (right of the ball). You'll see a banner of programs currently running. BlackBerry Messenger, Phone, Messages, PPT, Browser, and Home Screen will always be listed. Close any other by scrolling over to it, release the "ALT" key, then press the menu key, scroll down to "Close", and close that program to free up more memory for the others.

The red "end call" button only minimizes some programs so you can multi-task between them. Use the method above to make sure none are left running needlessly. - C. R.



"See what programs are running in the background by holding the "ALT" key, then press the back button..."

ABOUT RHODENIZER IT

We are a different kind of IT service provider. We don't sell any hardware or software. There are no sales incentives for steering you toward a particular product. We provide IT consulting services that include finding the best deals on what you really need and passing the savings along to you.

Our mission is to do more than fix computer problems.

Our mission is to help small companies save money, increase productivity, and safeguard private information.

We work with clients to prepare disaster recovery plans that ensure their critical data remains safe, yet easily accessible. The benefits of such strategic planning also includes money-saving ideas for managing resources and reducing IT expenses.

We have the training, experience, and know-how to provide the right solutions for your needs, and your budget.

Just call to schedule your **free initial consultation with no risk, and no obligation.**

Tell me about your computer needs or IT issues. I'll recommend a course of action that makes sense for your situation at no cost to you. What have you got to lose?

Rhodenizer IT
Information Technology Services

P. O. Box 768122
Roswell, Georgia 30076

(404) 202-8657

www.rhodenizer.com

The Rhodenizer Report is published and distributed by Rhodenizer IT, Inc. © Copyright 2007. All Rights Reserved.

DISCLAIMER: The information, opinions, and recommendations expressed within are for general knowledge and are not intended to be a substitute for personal consultation. Furthermore, some information may be based upon other information provided by third parties. Unless specifically stated, no form of independent verification is undertaken. The author is not responsible for any errors, omissions, or inaccuracies. This information is provided free of charge and is without warranty, neither explicit nor implied. The reader assumes all risk when performing any computer modifications without the direct supervision of a qualified IT professional.