



THE RHODENIZER REPORT

FEBRUARY 2009

www.rhodenizer.com

INSIDE THIS ISSUE:

IS THE INTERNET SAFE? 1

THE INEVITABLE WINDOWS 7 1

NEW VIRUS HIJACKS THEN WAITS 2

QUESTIONS FROM THE INBOX 3

BLACKBERRY TIP OF THE MONTH 4

ABOUT RHODENIZER IT 4

IS THE INTERNET SAFE?

When early American settlers headed westward across the plains into the wilderness it wasn't because they knew the journey would be safe. They weighed the risks versus the benefits and chose to take whatever precautions they could and proceed despite the dangers.

The Internet is not safe as long as it remains an unregulated "wild west" of anonymity and freedom. Whether this is good or bad can be debated in academic circles. The reality for those of us that go online and do business is that we are all responsible for our own safety.

Armed bandits, con artists, and "wild Indians" were the dangers the early pioneers had to be prepared for. Identity thieves, cyber terrorists, sexual predators, and anarchists are the modern day equivalent for us.

No website is safe. Even the commonly used "SSL certificates" used by online shopping carts can be forged. E-mails can be counterfeited, pop-ups with deceptive messages can come from websites you never even visited, and your own computer can be hijacked and used for criminal activities without you even being aware of it.

It's not difficult to defend your-



self against these threats if you know how. The real danger is in being unprepared and unwilling to learn.

A good defensive strategy has a plan for prevention and damage control. Prevention is about keeping bad things from happening. Damage control is about minimizing the damage in case they do. (CONT. P. 2)

THE TAKE-AWAY POINTS:

- **Internet is dangerous for those unprepared.**
- **Windows 7: What Vista was supposed to be.**
- **Windows updates are critical for the ongoing protection of your data.**
- **BlackBerry problems? Could be the battery.**

THE INEVITABLE WINDOWS 7

After the trials and tribulations that many early adopters of Windows Vista endured, the IT community at large has been anxiously awaiting a better alternative from Microsoft.

The answer finally came on Jan. 9th at 3:00PM when the beta version of Windows 7 was released for public download. The response was much greater than Microsoft had anticipated. People from around the world began overwhelming servers to

the point that Microsoft had to take them offline and postpone the event until capacity could be increased. This phenomenal excitement underscored just how desperate the public is for an alternative to Vista.

Now that we've had a chance to test it, reviews coming in echo many of the same sentiments. Windows 7 is not really "new", it's just an improved version of Windows Vista. **It's what Vista was supposed to be.**

While the experience of migrating to a new operating system will undoubtedly be better with Windows 7 than it was with Vista, there will still be a learning curve for those accustomed to Windows XP. Also, some applications may not be compatible so early research will be essential to a smooth transition. You may want to start planning soon since Windows 7 will most likely come on all new PC's by next Christmas. - C. R.

NEW VIRUS HIJACKS THEN WAITS

On Jan. 20th, Associated Press reported - "A computer virus that may leave Windows vulnerable to hijacking is spreading through the U.S., Europe, and Asia, infecting 9 million PC's so far. Finland-based F-Secure says it has been tracking this virus for weeks and has seen it surge more rapidly than anything they've seen in years.

Chief security adviser, Patrik Runald, said the virus's coding suggests it's a type of bug that may alert users to bogus infections on their PC's, then offer to sell them "antivirus" software that will remove it. "The gang behind this worm hasn't used it yet," Chief research officer, Nikko Hypponen said by phone. "But **they could do anything they like with any of these infected PC's at any time.**"

Also, Microsoft issued a secu-

rity update to deal with the so-called "Downadup" or "Conficker" virus, which appears to be a new version of a bug that appeared in October. "Over the last couple of weeks, a new variant of this worm has been affecting customers," the company acknowledged in a blog post. Microsoft said the virus is spreading by gaining access to one computer, then guessing at passwords of other users on the same network: "If the password is weak, it may succeed."

Most PC's with Windows will automatically download Microsoft's security update, but Hypponen said **the virus disables updates on infected machines.** While the origin of the virus is still a mystery, F-Secure surmises it came from Ukraine since it is coded to avoid computers there.

This may indicate that whoever wrote the virus is trying to not draw attention from their local authorities."

Cliff's Commentary: This is just another example of why it is so important to keep your antivirus software updated, and to make sure your PC is automatically downloading Microsoft's security updates.

If you are not able to check for Microsoft updates from within your IE web browser for any reason, there is cause for concern. These updates are critical for the ongoing protection of your network and the information it holds.

Infected PC's may not exhibit any symptoms until they are remotely activated as part of a coordinated attack. By the time you notice something is wrong, the damage may already be done.



"... the virus is spreading by gaining access to one computer, then guessing at passwords of other users."

IS THE INTERNET SAFE? (CONT.)

(CONT. FROM P. 1) Some **preventative measures** are:

A). Keep your antivirus protection updated. Most antivirus programs are supposed to update themselves automatically. But, I've seen instances where they stopped working and no one was aware of it. Check periodically to make sure.

B). Use another web browser instead of IE. Microsoft's

Internet Explorer has come a long way. But, it is still the most exploitable browser and the most vulnerable to attacks. Mozilla Firefox, Apple Safari, and Google Chrome are all preferable.

C). Be suspicious of any pop up messages you see. Don't assume the source is trustworthy unless you can confirm it by another means.

Damage control measures

can be as simple as:

A). Back up your files to a separate location regularly. If you don't know how, get someone to show you a way that you can then do yourself.

B). Get a back-up PC. Have it ready to go quickly in case your primary business PC becomes unusable. Parts are cheap, time is expensive.

Invest in some user training. Ask questions. Be prepared.



QUESTIONS FROM THE INBOX

Q– “I recently had to deal with the ordeal of having my identity stolen. What can I do to prevent this from ever happening again?”

A– Sorry to hear that. I’ve been there too so I know what a pain it can be.

To answer your question, there are a few things you can do to keep your private information from being stolen *directly* from you. But, there’s nothing you can do to keep it from being stolen from the many other sources where it can be found.

Keep your PC as secure as you can. Shred all your papers before throwing them away. Have your mail delivered to a locked P. O. box instead of your street mailbox. Use wash-resistant gel ink pens for writing checks, and never disclose anything about yourself over the phone to a caller you don’t know personally. Practices like these minimize our risk and make it harder for the unsophisticated thieves.

Unfortunately, this does nothing to protect the information about us in the many databases on many servers belonging to insurance companies, banks, healthcare providers, government agencies, schools, and online stores we’ve done business with in the past. Most modern day attacks are being launched against targets such as these

in order to score thousands of identities at a time and sell them on international black markets.

To protect yourself against that, all you can do is monitor your credit report, your bank statements, and your credit card transactions. Change your passwords from time-to-time and report any suspicious activity promptly.

Q– “Do you have some rule of thumb to determine when business computers should be upgraded or replaced?”

A– I’m not one of those “every 3 years” advocates, if that’s what you mean. You should only upgrade or replace assets when there is a compelling reason to do so.

The needs of your business should drive the IT solutions. Those solutions may require new procedures, new applications, or consolidated resources that require some capital investments. If your business is growing it makes sense to expand your ability to handle it.

However, if you’re like most small business owners right now, your priority is finding ways to cut costs and do more with less. If your present systems are adequate, keep them running in top shape. If you’re having problems with something that normally suits your needs, it

usually makes more sense to just get it fixed.

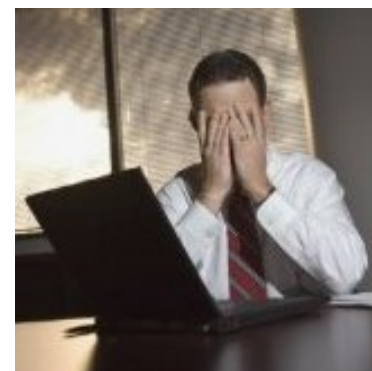
Only if your present IT assets (working properly) are no longer adequate to accommodate your business needs would it be wise to replace them. The most prudent thing to do in that case is to talk it over with an IT pro and get a recommendation for how best to proceed. You could save a great deal in the long run by having a sensible upgrade plan to follow.

Q– “I have a DVD that won’t read properly. Looks like dirty fingerprints on the bottom of the disc. What is the safest way to clean these?”

A– Mild dish washing liquid soap with a soft sponge and warm water. Then, rinse with cool water and dry with a lint-free towel. Avoid any excessive heat that could melt or distort the plastic.

The data on all DVD’s and CD’s is read by laser light. No magnetic material is used. It’s perfectly safe to get them wet as long as they are dry before you insert them in the player. Be careful not to use anything that may scratch or cloud the plastic as this may interfere with the laser light.

E-mail your questions to:
questions@rhodenizer.com



“...if you’re like most small business owners right now, your priority is finding ways to cut costs and do more with less...”

**TuneUp
Utilities 2009**

**Intelligent
Optimization
for your
Windows PC.**



Download from the
“Cliff’s Pick’s page
of my website.

Start your
free trial now!

BLACKBERRY TIP OF THE MONTH

Like many of my clients, I depend heavily upon my BlackBerry Curve 8310. The phone, e-mail, and GPS features are the most important to me on a daily basis. So, when it started having problems lately, it became a high priority for me to get them resolved.

It had been sluggish and occasionally locking up. Several times I had to remove the battery and reset it. Then, I noticed that almost every phone call was being interrupted by a loud buzzing noise in the background that would begin about 30 sec-

onds into the call. This would happen even while still connected to the charger and showing a fully charged battery. Since no one repairs these anymore, I assumed that an expensive replacement was inevitable. I was looking forward to upgrading to the BlackBerry Bold later this year, but I didn't want to just yet.

The solution came when I read some posts in a technical forum that discussed similar issues relating to a bad battery. Could it be that simple? Fortunately, the culprit revealed itself shortly

afterwards. I left the house that morning with a fully charged battery and it froze up on me again. After removing the battery, then re-installing it, the screen showed it as being nearly dead. I knew that was impossible, it had to be giving a false reading.

About \$40 later, I had a new fully charged battery and all of the previous problems are now gone.

THE TIP: Batteries can cause some flakey problems. Just because your battery shows a full charge, doesn't necessarily mean it's OK. - C. R.



ABOUT RHODENIZER IT

We are a different kind of IT service provider. We don't resell any hardware or software. We find the best deals on what you need and pass the savings along to you.

Our mission is to help small businesses reduce expenses, increase productivity, and safeguard private information.

It's about more than just fixing computers. We also

provide IT consulting and services that include finding the best solutions to your business problems.

We work with clients to prepare disaster recovery plans that ensure their critical data remains safe, yet easily accessible. Additional benefits include money-saving ideas for managing your computer resources and planning for future business expansion.

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 2009. 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.