

THE RHODENIZER REPORT

OCTOBER 2007

www.rhodenizer.com

INSIDE THIS ISSUE:

FREE ONLINE DOCUMENT SHARING	1
THE DANGERS OF P2P SHARING	1
WHAT'S IN YOUR LAPTOP?	2
QUESTIONS FROM THE INBOX	3
SECOND THOUGHTS ABOUT WINDOWS VISTA	4
ABOUT RHODENIZER IT	4

THE TAKE-AWAY POINTS:

- Use Google's online applications for free.
- P2P software on your PC can be dangerous.
- Safeguard portable files using encryption.
- Fewer companies now planning to upgrade to Windows Vista.

FREE ONLINE DOCUMENT SHARING

I don't have a crystal ball. But, based upon my experience in IT I think the future of software applications will look a lot like what Google is doing now with Google Docs & Spreadsheets. This is a free web-based word processing and spreadsheet program that allows you to create and edit documents from anywhere and collaborate with multiple people at the same time. Coordinate group homework assignments, access to-do lists from work or home, or work with remote colleagues on a project. You can import existing documents and spreadsheets, or create new ones from scratch. To invite people to view or edit a document, simply add their email addresses to the list of viewers or

collaborators. Take a peak at how a document is shaping up, or contribute your thoughts to a draft in progress. Keep track of multiple versions of the same document in one place with an easy drop-down menu that shows who changed what, and when. If you would like to keep a copy on your hard drive, you can export to a number of popular formats (DOC, XLS, ODT, ODS, HTML, PDF, etc.). Or, publish your work to an Internet web page or blog.

Google Apps provides some impressive communication and collaboration tools including email with your own domain name and up to 10GB of storage per account. It's all hosted online by Google, so there's no hardware to buy or software to



download. If you don't have an internet domain name yet, they help you register one when you sign up for an account.

The only down-side I can see is that you are trusting Google to keep this data secure on their servers. It may be fine for some uses and risky for others. User discretion is advised. To learn more about it, check out <http://documents.google.com>

THE DANGERS OF P2P SHARING

Last month, the FBI arrested a Seattle man for committing identity theft and fraud using information he harvested from music and file sharing (peer-to-peer) networks. Federal officials claim Greg Kopiloff used P2P software (such as [Kazaa](#), [Sharezaa](#), [LimeWire](#), [BearShare](#), [Morpheus](#), [Soulseek](#),

[and FastTrack](#)) to access personal information he found on other PC's running the same software. He is alleged to have fraudulently obtained \$73,000 worth of merchandise using the stolen identities of 83 people who had P2P software running on their computers. Kopiloff allegedly used income tax re-

turns, student financial aid applications, credit reports, and other data found on the PC's of unsuspecting users.

This case is just one example of how music and file sharing networks are treasure troves for identity thieves and potential terrorists. (cont. on P.2)

THE DANGERS OF P2P SHARING (CONT.)

(cont. from P. 1) P2P networks are intended to let users share music from a particular folder on their PC. The P2P software makes the folder available to anyone in the world using the same software. If care is not taken to configure it properly, it's easy to share not just the contents of that folder, but of the entire PC.

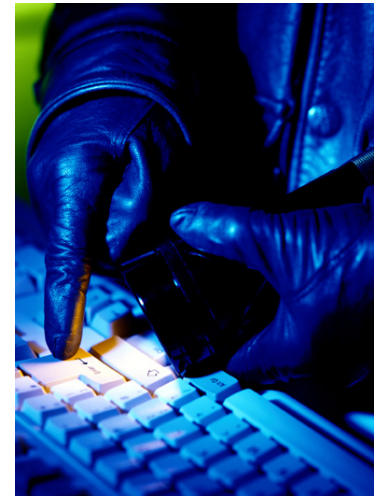
A study by Dartmouth College earlier this year showed that personal data is increasingly

being mined on P2P networks. Analysis showed a large number of searches aimed at uncovering financial data instead of finding music.

In July, the U. S. House Committee on Oversight and Government Reform heard testimony from witnesses, including Gen. Wesley Clark (ret.), about how everything from classified military documents to corporate data is freely available on music and file sharing networks. Items

found included the Pentagon's secret network infrastructure diagram, tactics used to defeat IED's in Iraq, and terrorism threat assessments for major U.S cities.

My 2 cents: If you find any of these programs on your PC, remove them and scan for spyware. Give the kids a separate PC to play with if you want to allow music sharing, and don't allow anything else on it that you wouldn't want to be made public.—C.R.



WHAT'S IN YOUR LAPTOP?

I find it curious that some people who carry very little cash on them for security reasons also carry around laptop computers with private information that would be a gold mine to ID thieves.

The greatest advantage of having a laptop is mobility, i.e., taking your work with you wherever you go. However, mobility also puts your confidential data at risk of loss or theft. All the money you spent on security for your office network is wasted if you carry the information outside with you unprotected.

Laptops are taken on trips, left in cars, and used in public places such as Internet cafes. Businesses lose millions of dollars each year due to the repercussions of lap-

top theft or covert wireless access. These problems can be avoided by either:

A). Leaving the data in a secure environment and accessing it remotely, or

B). Encrypting files locally to prevent unauthorized access.

Solution (A) provides superior protection against data loss and unauthorized access. You can also use another computer if yours becomes unavailable. But, this solution requires a constant Internet connection.

Solution (B) does not require Internet access. But, it only protects against unauthorized access. Protection from data loss depends upon your diligence in backing up files regularly and storing those

backups in a separate location.

Which solution is right for you? Several factors must be weighed. I can setup a single-user remote access solution for less than \$200 in most cases. 3rd party encryption products to protect the data on your laptop can be obtained for less than \$70.

Kensington has a product called PCKey (shown right) that provides 128 Bit AES hard drive encryption. The tamper-proof USB device and software work together as a laptop key. If you don't insert the key AND enter the correct password, you can't access the contents of the hard drive (\$69.99). For more info, go to <http://us.kensington.com/html/6331.html>.

"... all the money you spent on security for your office network is wasted if you carry the information outside with you unprotected."



QUESTIONS FROM THE INBOX

Q– “When I install software applications they usually prompt me to “register” at the end. Should I do this? How does providing my information to them benefit me?”

A– It doesn't. Most software companies will tell you that being in their database entitles you to receive product updates, or it makes you eligible to win something. It's actually a clever way of putting you on their marketing lists. Some even sell their lists to other companies. No legitimate business should ever require you to give your contact information in order to use a product you've already paid to use. You may have to register in order to receive something additional, but that's another transaction. When you purchased your software (or a license to use it), your transaction took place at the cash register.

Q– “On my computer, under “Add or Remove Programs”, there are some programs that I didn't install and don't recognize. Can I remove them?”

A– Only if you are sure they don't serve a purpose. Most new computers come with an assortment of “crapware” installed that can be, and should be, removed. However, there are legitimate device management programs (for laptop touch pads,

built-in wireless radio, or battery power-savings) that you don't want to remove. I would recommend doing a Google search on each program to learn as much as you can before deciding to remove it. Better safe than sorry.

Q– “My computer sometimes hangs for several minutes with the hourglass on the screen when I try to access a folder on our server. We removed lots of spyware and programs that were running in the background but it still happens. What else could be causing this?”

A– Those symptoms usually mean your computer is waiting for a response from another computer, or process. Since it only happens when you select a certain resource, it stands to reason that the resource is not responding in a timely manner. Why? The first step is to find out if anyone else on your network has the same problem. If so, it's probably something you both have in common. If not, the culprit may be on your end.

An experienced IT consultant with a good network analyzer should be able to take some readings and identify the source of the problem for you. I use a One Touch Series II Network Assistant by Fluke. It runs a thorough test and produces comprehensive reports in just a few minutes.

Q– “I bought a Linksys router and installed it myself. It seems to be working fine but how can I know if the security is setup correctly? Is there an easy way to test it?”

A– Yes. Go to Steve Gibson's website at www.grc.com and look for “ShieldsUp”. It's an automated system created as a free diagnostic tool to look for security vulnerabilities. It even makes suggestions for fixing common problems. There's nothing to install, just follow the instructions on the webpage. I've been using it for many years and consider it a trustworthy resource.

If your router ports are tested and found to be in “stealth mode”, you get a passing grade and peace of mind knowing you are as protected as you can be from a random attack. If you get a failing grade, it suggests corrective actions that you can attempt to do yourself, or call an IT pro to handle for you.

Either way, it's a free test and you'll have a better idea of how effective your home or office network security measures really are.

Send your questions to:
questions@rhodenizer.com

If we use your question in one of our newsletters, we'll send you a free Rhodenizer IT stainless steel travel mug.



“... An experienced IT consultant with a good network analyzer should be able to take some readings and quickly identify the problem...”



SECOND THOUGHTS ABOUT WINDOWS VISTA

According to a survey of IT administrators by PatchLink in July, fewer businesses are planning to upgrade to Windows Vista now than when a similar poll was taken last December.

Of 253 clients surveyed, 2% reported running Vista, 9% said they plan to, and 87% said they were sticking with Windows XP. Compare that to last December when over 43% said they planned to upgrade to Vista and only 53% planned to wait. When asked about their confidence in Vista's security, 50% said they believed Vista to be

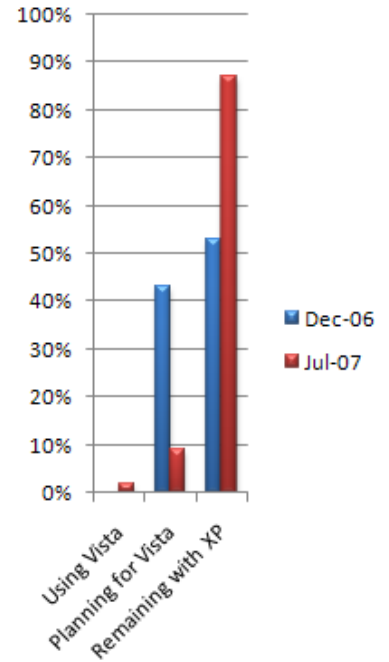
more secure than Windows XP. 15% didn't believe so, and 35% weren't sure. However, the most recent poll reveals only 28% now believe Vista is more secure while 24% disagree, and the unsure climbed to 49%.

Reconsidering Vista has given rival operating systems a new shot at breaking into small business markets. Last year, Linux and Mac had only meager appeal with 2% planning to try Linux and none with plans for Mac OS X. July's survey, however, noted a substantial increase in the total number willing to dump

Microsoft Windows on at least some systems. 8% of those polled acknowledged Linux plans, and 4% said they will begin to deploy Mac OS X.

PatchLink's survey results seem to support what other forecasts from research firms are also indicating. Widespread adoption of Windows Vista by businesses won't seriously take hold until early 2008, and probably after the release of the anxiously awaited "Vista Service Pack 1" update.

My advice? Save your money. Don't upgrade unless there is a compelling reason to.—C. R.



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 at all times. Benefits of such strategic planning also include 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 IT problems or concerns. Let me recommend a course of action that makes sense for your situation. I'm betting my time that you'll be impressed.



P. O. Box 768122
Roswell, Georgia 30076

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.