



THE RHODENIZER REPORT

JUNE 2007

www.rhodenizer.com

INSIDE THIS ISSUE:

HOW YOU CAN REDUCE SPAM EMAILS	1
THE ULTIMATE SPAM KILLER	1
HOW YOU CAN REDUCE SPAM (CONTINUED)	2
THE ULTIMATE SPAM KILLER (CONTINUED)	2
QUESTIONS FROM THE INBOX	3
WIRELESS SECURITY TIPS	4
ABOUT RHODENIZER IT	4

HOW YOU CAN REDUCE SPAM EMAILS

Anyone with an email address will inevitably receive unsolicited emails, or SPAM. It's just as unavoidable as junk mail. However, there are steps you can take to greatly reduce the hassle and annoyance.

#1—Keep your primary email address private.—“Spammers” use programs called “crawlers” to search websites across the Internet and collect email addresses. If your email address is posted on any web page, it's only a matter of time before it's picked up and added to email marketing lists. If you discover your email address visible on a public website, ask the manager of that website to make it a “masked email link” so it will only be visible when a person hovers or clicks on it.

If you have your own domain name, you can create email “aliases” (email addresses that secretly forward email to your address without revealing it) through the control panel provided by your online hosting account. These are useful for “one-time” purposes such as shopping, registration, or whenever incoming message won't need a reply. Messages sent to these aliases are forwarded to your primary email. Just be aware that if you reply, it will reveal your primary address to that recipient. If SPAM begins flooding in via one alias, you can just delete it and all subsequent messages will bounce back to the sender.

“Disposable” email accounts are another option. You can



sign up for a free email account with Yahoo, Hotmail, Gmail, or any of the other free providers. If one of these email addresses gets picked up by “spammers”, just close the account, open another account, and send your friends the new address. Unfortunately, this is not a practical solution for business. When you have distributed printed materials with your company email address, you can't hide. But you can fight back (continued P. 2)

THE TAKE-AWAY POINTS:

- SPAM is unavoidable but can be greatly reduced.
- If you host your own email server, it's not just a nuisance. It's a business risk.
- SPAM firewall solutions are best.

THE ULTIMATE SPAM KILLER

The above article contains general guidelines that apply to home and small business users. However, businesses that have their own email servers are at risk of far more than just the mere inconvenience of daily SPAM. They risk having their server hijacked and used remotely to deliver SPAM to the

rest of the world (I've only seen this personally in a couple of cases, but it's not uncommon in small companies where no proactive monitoring exists). Before you realize what's happening, your company domain name can be “blacklisted” because of all the SPAM coming from it and your outbound

emails blocked by your Internet Service Provider. It can be a very difficult and time consuming process to recover from. Some ISP's take SPAM very seriously and will not “un-block” you until the problem has been resolved and your server and domain records meet certain standards. (continued P. 2)

THE ULTIMATE SPAM KILLER (CONTINUED)

(cont. from P. 1) Fortunately, there are ways to prevent such problems. The ultimate solution for some is the SPAM Firewall from Barracuda Networks.

The Barracuda Spam Firewall is an integrated hardware and software solution for complete protection of your email server. It provides a powerful and easy to use solution for eliminating spam and viruses. Compatible with all email servers, it handles

up to 30,000 email users on one network. No software to install. No modifications required to existing email systems. It also has a web interface for monitoring and maintenance. With “Energize Updates”, the Barracuda Spam Firewall is continuously updated with the latest spam and virus definitions every hour - keeping maintenance at a minimum and eliminating administrative overhead. Updates are provided by Bar-

racuda Central where engineers work around the clock monitoring the Internet for spam and virus threats.

There are several models to choose from and prices start at around \$1500.00 for the basic model. This truly is a “set it and forget it” device that can plug into any existing network. While it may be a bit pricey for some, I would consider this the “Ultimate SPAM killer” for small businesses serious about SPAM.



SPAM FIREWALL

HOW YOU CAN REDUCE SPAM EMAILS (CONTINUED)

(cont. from P. 1) in other ways.

#2—Use SPAM filtering.-

Many website and domain hosting providers include virus and SPAM filtering in their website packages. There are also online services (such as [MailWise](#) and [AppRiver](#)) that intercept and filter out SPAM for a fixed monthly fee. You can even setup your own system to filter out SPAM using software such as [SPAM assassin](#), but the setup and maintenance can be a burden.

#3—Don’t buy products or visit websites promoted by SPAM emails.— Doing so only encourages more. If they aren’t making any money, they’ll stop doing it. One of my primary rules of Internet

commerce is: “Never do business with anyone you can’t track down & locate.”

#4—Report Offenders. -

Unfortunately, many spammers operate either on foreign soil, or by using “drive-by” connections to the unsecure Wi-Fi networks found in almost every Metro area neighborhood. This makes them almost impossible to find. But, if they can be identified, complaints can be filed with the Federal Trade Commission at www.ftc.gov.

Some companies are simply trying to offer their products and/or services by email advertisement. There is nothing immoral or illegal about it as long as they comply with the [U.S. CAN-SPAM Act of 2003](#). In short, the law states

that senders must not conceal their identity. They must include their mailing address in the email, and they must provide you (the recipient) a means by which you can “opt-out” and be removed from their email marketing list. Violators face fines of up to \$11,000 per occurrence.

Legitimate businesses will gladly comply with “opt-out” requests since they don’t want to annoy anyone they may potentially do business with one day.

“Spammers”, on the other hand, get paid to blast messages to numbers of “live” addresses. If you reply asking to “opt-out”, it only serves to verify that your email address is a “live” one so you’ll soon receive even more SPAM.

“many spammers operate by using “drive-by” connections to the unsecure Wi-Fi networks found in almost every Metro area neighborhood..”

QUESTIONS FROM THE INBOX

Q—Why do I sometimes get emails with random words that don't make any sense?

A— The words are only intended to fill up space. These emails are “shots in the dark” to see if anyone is there. Automated programs randomly choose email addresses. If the message doesn't bounce back to them, it's assumed to be a valid email address and added to a list that can be sold to email marketers. There's nothing you can do but delete them.

Q— Which is the safest web browser for me to use?

A— I can tell you which one to avoid: Internet Explorer version 6 or below. Microsoft made significant security improvements with IE v. 7. But, older versions have been plagued with vulnerabilities. Firefox was my favorite until IE7 came out. Now, they are both fine choices. Whichever one you choose, make sure you keep it updated.

Q—What's the best way for me to backup all my data?

A— That depends upon several factors. You must consider how many PC's, how many applications per PC, and where those applications store data. Then, determine the total amount, and how often it should be backed up.

Lastly, where can backups be stored safely? Do you want to handle the routine yourself, or pay to have it automated?

From USB flash drives, to an online backup service. Many options are available. If you aren't sure which is best for your needs, consult with an experienced IT pro.

Backups are also a key part of creating a disaster recovery plan. Backing up your data is no more important than being able to recover it after a disaster. A disaster recovery plan is the cheapest business insurance you can buy.

Q— Should we upgrade to Windows Vista? What about Office 2007?

A— Not unless you have a compelling reason to do so.

There were earlier versions of Windows and Office that I couldn't wait to get away from. But, not this time. Office 2003 is still a viable product (as you can tell by prices remaining nearly even with Office 2007). And Windows XP Pro, SP2, has matured into the most stable and secure version of Windows yet (with all the latest updates installed).

Vista and Office 2007 have been out since February, but most companies aren't rushing to upgrade. They see no business justification for it...

no return on investment. Some new features are nice, but not all changes have been well received.

I attended the Microsoft launch event earlier this year and spoke with other IT pros who agree that every new version of Windows and Office since '95 has had problems in the initial releases. Most were resolved in the Service Packs that came out within a few months. So, if you really want to upgrade, at least wait for Service Pack 1.

Q—How can I speed up my computer without spending a lot of money?

A—Relieve some of the burden on the PC, and add more memory (at least 512 MB). Prices are lower than ever so it's a great time to upgrade.

The leading causes of excessive PC burden is spyware and drive fragmentation. Alternate between Spybot and AdAware SE to scan for spyware. Advanced users can also try the trial version of [TuneUp 2007 Utilities](#), followed by the “Disk Defragmenter” (Start, All Programs, Accessories, System Tools...)

Download the free programs mentioned above from the “Cliff's Pick's” page on [my website](#) www.rhodenizer.com.

Send your questions to: questions@rhodenizer.com



“Backing up your data is no more important than being able to recover it after a disaster.”

IBackup
Flexible Storage Solutions
securely backup and restore files with encryption, compression, scheduling and a host of other features.

Download the free programs mentioned above from the “Cliff's Pick's” page on [my website](#) www.rhodenizer.com.

Send your questions to: questions@rhodenizer.com

WIRELESS SECURITY TIPS

So, you bought an inexpensive wireless router. Setup was easy, wasn't it? You can now connect to the Internet from anywhere in the house or office. Even out on the patio, right? What you may not realize is... so can everyone else in your area.

Most don't see this as a big deal. At least not until I enlighten them to the potential dangers. It's not just a matter of protecting your PC's from intrusion (though that's part of it). It's also an open invitation to criminals who cruise around looking for open wireless access. This

gives them the ability to launch SPAM and viruses to the Internet using your IP address. If investigated, the trail will lead back to your home or business. Your Internet service may be cut off, or you may be visited by law enforcement agents with lots of questions. The best way to avoid this is to secure your wireless network against unauthorized access.

Using the web based control panel you used to set it up, go back and make these changes:

1). **Choose a wireless encryption method.** WPA2 is best.

WEP is... better than nothing. Use the highest level your router and all connecting devices will support.

2). **Turn off SSID broadcast.** Once you've established a connection, you don't need to continually advertise it.

3). **Enable MAC filtering.** This is a setting that enables you to "register" devices on your network. PC's not on the list can't connect—even with the correct password.

These measures will make your wireless network much more difficult to hack, and more likely to be passed over for easier access elsewhere.



ABOUT RHODENIZER IT

Rhodenizer IT is a different kind of IT service provider for the north Metro Atlanta area.

We sell no hardware or software. We have no quotas or markups. We provide consulting services that include finding the best deals on what you need... and passing the savings along to you.

We also provide complete service for business computer networks, but our mis-

sion is not only about fixing computers. It's about solving your IT problems in a way that will save you time and money... guaranteed.

We also help companies create strategic plans for reducing their IT costs and increasing the security of their most vital asset: Information.

A well organized IT operation will save your business time and money in the long run.

Let us show you how... at no cost to you!

Call for your **free initial consultation with no obligation.** Tell us about your IT problems and concerns. Let us recommend a course of action. It costs nothing to find out if we have the answers you need.

"Client satisfaction is just not good enough. I won't rest till you're impressed!" - C.R.

Rhodenizer IT
Information Technology Services

RHODENIZER IT, INC.
P. O. Box 768122
Roswell, Georgia 30076

Email: info@rhodenizer.com
Phone: 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 supervision of a qualified professional.