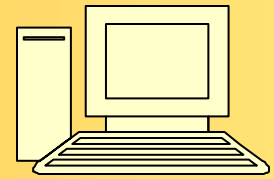


BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.



Newsletter

Issue 9

September 2010

23rd Year of People Helping People!



In this Issue

Websites to avoid	2
Internet Security best...	3
Set Hacker alarm	4
Malwarebytes information	5
Malwarebytes inform. <i>Cont.</i>	6
More about Internet threats	7
How to stop Spam	8
Enlarge print	9
Enlarge print and resolution	10
The lighter side	11

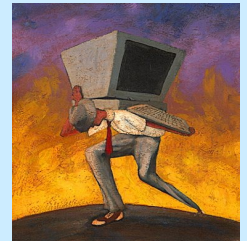
Don't forget to visit our club's site at:

<http://gtbpcug.org>

<http://www.smartcomputing.com>

The Wired vs. Wireless Debate

To wire or not to wire, that is the question commonly asked by users who want to build home networks around their media-ready PCs. Unfortunately, there's no easy answer.



The fact is that a hardwired Ethernet network offers unbeatable speed, steady reliability, and impenetrable security. Data shot across a coil of Category 5 or Category 6 (commonly referred to as CAT 5 or CAT 6) cable can travel at rates of "100Mbps (megabits per second) or faster. Better yet, it's immune to interference from microwave ovens and cordless phones.

The same cannot be said of wireless networking technologies, at least not at the present time. Indeed, when measured strictly by objective performance standards, "802.11a/g" proves a weak alternative to the far-superior Ethernet. But performance may not be the most important issue to consider when building a home network around a media ready PC. In fact, it may not be an issue at all. Network speed may not matter to you if your home network is small or tightly knit; if you rarely use the network to transmit video files to other computers; or if the video files you transmit are highly compressed, brief in duration, or saved at a low resolution.

Ditto if a network upgrade would require you to dig into the walls. Whether a person should implement a wired or wireless network to complement a media-ready PC depends on many things, including the user's intentions and expectations, the configuration of the home entertainment system, and the condition of the house.

What's right for one person may not meet the needs of someone else. We advise you to consider your home entertainment needs; review the system requirements of your multimedia hardware (some streaming video devices require an Ethernet connection, while others do not); and make a decision that works with your existing equipment, fits into your budget, and satisfies your individual performance expectations.

<http://www.urlvoid.com/>



From Kim Komando's newsletter

<http://www.komando.com>

Sites you better stay away from

Here is the list of the most detected domains and subdomains, analyzed in [URLVoid](http://www.urlvoid.com/) during these first two weeks. This list was created with the counting of domains detected by at least 9 engines, and we can see that the most dangerous domain is detected by 12 engines.

In the list below, there is the country code where the domain is hosted, the domain name, the IP address of the server where is hosted the domain and the number of the engines that detected the domain.

-  xxxtoolbar.com (66.152.93.119) (12 DETECTIONS)
-  spywarebot.com (174.123.38.26) (11 DETECTIONS)
-  install.xxxtoolbar.com (66.152.93.119) (11 DETECTIONS)
-  aroolohnet.ru (77.78.240.24) (11 DETECTIONS)
-  russianmomds.ru (59.53.91.195) (11 DETECTIONS)
-  spyeye100.org (88.208.252.193) (10 DETECTIONS)
-  kolpredv.com (77.221.153.141) (10 DETECTIONS)
-  xorg.pl (94.23.1.180) (10 DETECTIONS)
-  zerovir.com (85.12.46.203) (10 DETECTIONS)
-  zief.pl (91.188.59.197) (10 DETECTIONS)
-  d0ma1ns.info (188.65.73.170) (10 DETECTIONS)
-  nevereversite.ru (194.140.229.101) (10 DETECTIONS)
-  fast-scanneronline.org (91.188.60.3) (10 DETECTIONS)
-  theautocompanyy.info (194.8.250.103) (10 DETECTIONS)
-  hjwbxhqr.cn (193.33.115.26) (9 DETECTIONS)
-  ophaeghaev.ru (97.101.146.174) (9 DETECTIONS)
-  parfaitpournous.com (200.115.112.222) (9 DETECTIONS)
-  fnmaw.com (91.212.127.110) (9 DETECTIONS)
-  cquenceclothing.com (205.134.252.251) (9 DETECTIONS)
-  charter-x.biz (91.213.174.107) (9 DETECTIONS)
-  b00tlife.com (79.135.152.26) (9 DETECTIONS)
-  convart.com (213.163.89.55) (9 DETECTIONS)
-  threatnuker.com (72.44.67.7) (9 DETECTIONS)
-  vv00vv.biz (91.213.174.8) (9 DETECTIONS)
-  krclear.com (194.8.250.60) (9 DETECTIONS)
-  babah20122012.com (193.105.207.98) (9 DETECTIONS)
-  ramualdo.com (213.163.89.55) (9 DETECTIONS)
-  chura.pl (91.188.59.197) (9 DETECTIONS)
-  spywarestop.com (174.123.38.26) (9 DETECTIONS)
-  vrituyes.in (91.212.198.157) (9 DETECTIONS)
-  technology-scanner.com (195.5.161.211) (9 DETECTIONS)
-  adwarealert.com (174.123.38.26) (9 DETECTIONS)
-  vvmmp.ru (195.98.50.102) (9 DETECTIONS)
-  directupdate.info (91.188.60.10) (9 DETECTIONS)

In these first two weeks were analyzed a total of 43367 unique websites and 12394 websites (28.5 %) were detected by at least 1 engine.

Internet Security Best Practices

By Dave Palmer <http://www.techteachtoo.com>

Basics

There are no "safe" websites.

Use GOOD passwords where money or sensitive information is involved.

Physical Security

Keep your laptop with you at all times when not at home. Treat it as you would your wallet or purse.

If multiple people use one computer, create user accounts for everyone, including yourself.

(Only for Windows users, not for Mac users)

Unless you're a tech-literate power user, create a user account for yourself even if you're the only one using the computer. It will greatly reduce the risk of getting infected.

Browser Security

Watch URLs to know for sure where you are. Don't assume a website is what it claims to be unless you've typed in the URL yourself. Even then you might be wrong. Seeing the lock icon on the address bar or elsewhere on the page only ensures that the data is being transferred securely.

It doesn't ensure that the vendor is trustworthy or that the database of customer information is secure. Never type an important password (leading to money, sensitive information, etc) into a non-encrypted page (one without the lock icon). Delete cookies, flash cookies, adware and spyware unless you have a good reason to keep them.

Make online payments more secure

If possible make payments through a 3rd party like PayPal. Fewer vendors will have your credit card number. If you can't use a 3rd party for payment, use a credit card for online purchases rather than a debit card. Credit cards reduce the liability of the problem if something goes wrong.

Increase e-mail security

Be suspicious, if not paranoid, about e-mail attachments and websites. Don't allow your browser to remember your passwords.

Don't assume that any e-mail is actually from the "From" address.

Delete obvious spam without opening it.

Don't open e-mails with attachments unless you know what the attachment is.

Don't trust unsolicited e-mails.

Never click on links in e-mails. Type the URL into the browser yourself.

Final notes

Backup your data, or your whole system, regularly. There's a lot you can't defend against.

A backup of your data or computer will make recovery much easier.

Turn your computer off when not in use. Broadband and an always-on connection can be a dangerous combination.

Nothing is foolproof. Good security practices such as these don't eliminate the risk, but they make you less of a target.

Set Hacker Alarm on your Web Mail Box By Erik Larkin www.pcworld.com

Use a clever trick and free tools to find out if someone has been snooping into your e-mail to steal sensitive information.

Your Web Mail account is a treasure trove of private and potentially valuable information and thieves know it.

In an online interview, one publisher claimed to make thousands of dollars everyday by breaking into people's accounts and searching for messages that contain financial details (read more about this interview at (find.pcworld.com/57837)

Normally you can't tell whether you've been hacked in this way. Even if you cannily leave a juicy-sounding e-mail unread, a thief or snoop may read it and then return its status to unread. But with a little bit of know-how, you can create an electronic trip wire that will trigger whenever someone reads a rigged e-mail. I came across the idea, which takes advantage of a free Web hit counter, in a blog post by Jeremiah Grossman of White Hat Security (find.pcworld.com/57838). After I talked with him, we came up with a setup that's easier than the one he originally suggested.

The gist of it is to keep an e-mail message in your account that includes the code for the counter. Opening the attachment trips the counter, thereby alerting you that someone was snooping.

Here's how to set it up:

1. Head over to OneStatFree.com and register for a free Web counter account. You can list anything for the site URL, and use a disposable e-mail address to complete the registration process (find.pcworld.com/5783) for tips on using such e-mail accounts.

2. Look for an e-mail from OneStat sent to the address you used when you registered.

It will come with an attached file named OneStatScript.txt. Save that file, and note your account number.

Then delete the e-mail, which has your account details.

3. Give a text file a name that will catch a spy's eye, like "Bank Passwords," and make it an .htm file so it opens automatically in a Web browser (and trips the counter).

4. Send the file as an e-mail attachment to the Web mail account that you want to monitor. Use a similarly baited subject line, like "Account log-ins; for the message. Just be sure not to open the file when you send it-you don't want to set off your own alarm.

5. Sit back and wait like the patient spy-catcher you are. If anyone opens your rigged attachment, the hit counter will reflect that fact and will record information about them, including the IP address of the accessing computer.

To check the counter stats, just log back in to your account at OneStatFree.com. Of course, the way to maximize your protection is to avoid keeping sensitive financial data in your Web mail in the first place. The excellent, free Stanford Password Hash browser add-on (find.pcworld.com/57836) provides additional security by making it easy to use strong, unique passwords for all of your accounts.

IMPORTANT INFORMATION FOR ALL USERS OF MALWAREBYTES SOFTWARE

By Ron Hirsch - ronhirsch1439@comcast.net

Malwarebytes security software has been, and still is one of the best software programs available to help protect your system from the rash of malware and similar "bad stuff" out there in the computer underworld.

I have been using it in conjunction with Microsoft Security Essentials for quite a while now, starting with my older Windows XP Pro 32 bit system computer, and now with my new Windows 7 64 bit computer.

Malwarebytes comes in two versions, free and paid. The free version of Malwarebytes does not offer real time protection, but users can initiate a scan any time they want, to search for malware. The paid version is a lifetime license, with real time protection.

I recently learned that if you are using the paid version, and have set it for real time protection, there can be conflicts with your other security programs. But these conflicts can be stopped by listing the various Malwarebytes active files in the "exclusion" folder of your other antivirus/security software.

I discovered this by accident recently, when my copy of the paid Malwarebytes program notified me that a newer version had been downloaded. And, did I want to install it. Of course, I said OK, and that proceeded to close the program and then install the newer version. It then said I had to reboot, so I did.

After the machine had rebooted, everything was frozen solid, so I tried another reboot, but that also locked everything up tight. It seemed pretty obvious that Malwarebytes was the cause here, but what was the cure? I booted up using SAFE mode, and it booted OK. While in SAFE mode, I decided to just uninstall Malwarebytes, until I could find out the proper solution.

The next normal boot had everything working fine, no lockups - all was normal, confirming that Malwarebytes was the cause. So I sent an email off to Malwarebytes. They got back to me very quickly, and gave me this link below to explain the problem and solution to the freeze-ups.

<http://forums.malwarebytes.org/index.php?s=70b8be10374840dca65629a2162b6d60&showtopic=10138&st=0&p=167851&#entry167851>

If you are not running the paid version, with real time protection, then this fix may well not be needed. But for those using real time protection, it is mandatory.

This is a thread on the Malwarebytes forum, and someone has clearly presented all the fixes to solve the problem, with a wide range of antivirus programs. The fixes are applicable to most versions of Windows, but I believe that the paths for the fixes here are primarily for Windows 32 bit systems. The information presented contains screen shots for those who have problems understanding the fixes.

If you have any trouble accessing this link, I have, as I noted below, created a PDF file of this complete presentation, and it is available on the BRCS site, along with the PDF versions of my articles. See later for a link.

The file locations for 64 bit Windows systems are different. Below are the respective locations for Windows 7 64 bit. I have no other 64 bit systems, but I would guess that Vista's locations are probably similar. Since most of you will still be using a 32 bit operating system, such as XP or Vista, you will probably find that the file locations will be as shown on the Internet page, and in the PDF file I've created from the site.

But, you must be familiar with copying files in Windows Explorer to a specified location, depending upon your software. If you cannot do this, get a friend to help you.

Once you have located the target area of your antivirus software, you must then copy the files specified in the online (or PDF copy) of the instructions.

And, remember for 64 bit Windows versions, such as Windows 7 64 bit, the location of the files to copy is different.

Where you see C:\Windows**System32**\drivers\

You should use C:\Windows**SysWoW64**\drivers\

Where you see C:**Program Files**

You should use C:**Program Files (x86)**

Once I added to the exclusion window for Microsoft Security Essentials, all my problems were resolved. There were no freeze-ups at boot-up, and the freeze-ups of various programs during operation disappeared completely. So I have confirmed that the fix works just fine.

If you would like to download a copy to read, or save, of the info presented on the Malwarebytes site, please go to:

<http://brcs.org/hirsch.php>

which is our society's home page, and look for the file named Malwarebytes Info. You can read it online, and/or save it, as desired. And you can also download a PDF of this article, which is named "Malwarebytes article", if you'd like a copy for your records.

REMEMBER - Malwarebytes remains as one of the best security programs out there. I recommend it to all users. And for the small price of \$24.95 you will have lifetime free updates of the program and the malware database, and real time protection. If you will want to go with the free version, you will have free database update, and scans anytime you want.

Using this program, and Microsoft Security Essentials will afford you top notch protection.

Is Your Internet Security up to Date?

Antivirus up to date?

Firewall?

Windows up to date?

Spy Ware?

See how to protect your computer at:

<http://www.gtbpcug.org/protect/>



More about Internet Threats

By Dave Palmer <http://www.techteachtoo.com>

Who are the people sending spam and why do they keep doing it?

The answer to the 'why' part of the question comes down to one word: **money**. Very few sane people would send out millions of spam e-mail per day for the fun of it. It's about profit.

The 'who' part of the question is a bit more complicated.

A very small portion of spam is sent by legitimate businesses that don't understand or follow the 7 rules the FTC (Federal Trade Commission) laid down in the CAN-SPAM Act of 2003. They didn't intentionally set out to break the law but, through negligence, they did.

The rest of the spam that gets sent daily comes from criminals. These e-mails fall in 4 basic categories:

Infection Attempts – the idea here is to provide links and attachments in the e-mails. Clicking on the attachment will get you infected. Likewise the links will lead you to a website that will also infect your computer. The bad guys have thousands of clever ways to fool you or entice you to click on a link – any link. And the minute you do you're infected. Then your sensitive information is up for grabs. They may even attempt to control your computer remotely – to send out more spam.

Sales Attempts – The products are often drugs, jewelry or some type of body enhancement product. The prices are unbelievably low- for good reason. Many of these e-mails are simply a scam – there are no products. The rest are shoddy quality or altogether fake

Phishing Attempts – Phishing is an effort to convince you to give up sensitive information by pretending to be a legitimate organization or business such as a bank. If you are fooled into responding to these requests, your identity and money will often be stolen.

Scam Attempts – These e-mails are an effort by criminals to begin a conversation. They attempt to do this by spinning a story that hooks you with curiosity, greed compassion or other emotion. Once the conversation begins, they will spin more stories, and use promises, threats or anything else to convince you to send them money for one cause or another.

The bottom line is that it's all about money. The fact is that these criminals are using our computers to send billions of spam messages a day. It really doesn't cost much more to send 10 billion per day than it costs to send 1 billion. So the question from the spammers point of view is 'Why not?' If they get a response of 1/10th of 1% on 1 billion spam then for very little extra cost or effort, they can multiply their profit 10 times by simply sending more spam.

By Dave Palmer <http://www.techteachtoo.com>

How to Stop Spam – The First Step

This post is the first in a series about how to stop spam.

There's no denying that e-mail spam has grown to be a huge problem and a serious threat. It seems spam is completely out of control. So what's being done to get a handle on it? What can you do to limit the spam you receive?

The first step in stopping spam is to understand exactly what spam is.

Most people would say spam is "e-mail I don't want." But there are some problems with that definition. First it's not the legal definition. Second, that definition makes Aunt Betty a spammer when she forwards yet another chain e-mail about cute kittens or "you must send this to 15 others to insure world peace."

Let's start with the legal definition of spam. In 2003 the U.S. government and the Federal Trade Commission (FTC) created the CAN-SPAM Act, also known as the Controlling the Assault of Non-Solicited Pornography and Marketing Act. At that time spam made up about half (50%) of all e-mail sent. Today it's estimated that 90%-95% of e-mail is spam. I saw one estimate of the volume of spam put at 17 billion, yes billion, PER DAY! That's unbelievable.

According to the FTC, "...the CAN-SPAM Act doesn't apply just to bulk email. It covers **all commercial email**..." It also "...makes no exception for business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law." Aunt Betty's e-mails aren't spam because they're not commercial. But her e-mails are still a problem and a potential threat. More on that in another post.

According to this FTC page <http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm> **all commercial e-mail**, including bulk e-mail, must comply with the law in 7 areas:

- 1) The company cannot use false or misleading header information. The "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
- 2) They cannot use deceptive subject lines. The subject line must accurately reflect the content of the message.
- 3) They must identify the message as an ad. The law gives them some leeway here, but the notice must be clear and conspicuous.
- 4) They must tell you where they're located. The message must include a valid physical postal address, whether it's a street address, a post office box or a private mailbox with a commercial company.
- 5) They must explain how to opt out of receiving future email. Again, it must be clear and conspicuous and "...easy for an ordinary person to recognize, read, and understand."
- 6) They must honor opt-out requests promptly. In this case promptly means within 10 business days. Several other conditions apply including one that says the business can't sell or transfer your email addresses, even in the form of a mailing list.
- 7) They must monitor what others are doing on their behalf. That means if they hire another company to handle their email marketing, the original company is still responsible for complying with the law. If there are problems both companies may be held legally responsible.

This law means that commercial or business bulk e-mail is not spam, unless it violates the rules above. Legitimate businesses will comply with the above rules. Those that don't are sending spam and are illegal.

Submitted by member Gary Staley

Enlarge print when printing from a Webpage

By The Computer Lady <http://asktcl.com/>

Dear Computer Lady,

I like to print things out occasionally from Internet sites (example: my bank activity), and I have tried every trick I can think of to make it print larger. I increase the size on the screen, but when it prints, it always comes out tiny, hard to read. I've tried saving a screen to Word, increasing the size of that page, and printing it out. No matter what I do, I can't make it larger, including by telling printer to "fit to page," which in many instances should enlarge what's on it.

What can I do to get a larger, more legible printout?
Thanks for all your help.

Marianne

Dear Marianne,

This is a fairly common question.
Let me start by explaining a common misconception.

When you enlarge the view on your computer screen, you are not changing the size of the actual document. This is true both on web pages which you are asking about, and in documents like Word. From your description, I suspect that you are increasing the size of the text on your monitor, but not in print settings. The good news is there is another way to change the actual printed size in some programs.

I normally use Google Chrome to surf the web, and there are no settings to change the size of your printed output. You did not say what web browser you are using, so I decided to look around and see if there are any other options out there.

I found that you can indeed change the print size in Internet Explorer 7 and 8, as well as Mozilla Firefox. You just need to use the "Print Preview" dialog to do so.

When you are at a page you want to print in Internet Explorer, click on the drop-down arrow to the right of the printer icon, then click on "Print Preview..." In the print preview window, there are two drop down lists, one is for the number of pages you want to preview at a time, and the second is for the size you want your page to print. The first option is "Shrink to fit".

Click on this drop down list, and experiment with the different settings until you find the one you like. They range from 30% of the original page size, up to 200%.

You can also change the paper from portrait to landscape, to see if this will help make the pages more readable.

Once you have the size you want to print, click on the printer icon on the left of the toolbar and print your pages.

I was able to use this method to print articles off my website in really large print.
I hope it works for you as well.

Elizabeth

From the Adobe Photoshop Elements Help file

Change print dimensions and resolution without resampling

You might need to change the print dimensions and resolution if you are sending the image to a print shop that requires that files be at a specific resolution.

If you are printing directly from Photoshop Elements, you don't have to perform this procedure. Instead, you can choose a size in the Print dialog box and Photoshop Elements applies the appropriate image resolution.

Note: To change only the print dimensions or the resolution, and adjust the total number of pixels in the image proportionately, you must resample the image.

1. In the Editor, choose Image > Resize > Image Size.
2. Make sure that Resample Image is deselected. If deselected, you can change the print dimensions and resolution without changing the total number of pixels in the image, but the image may not keep its current proportions.

Note: Resample Image must be selected in order to use the Constrain Proportions and Scale Style functions,

3. To maintain the current aspect ratio, select Constrain Proportions. This option automatically updates the width as you change the height, and vice versa.
4. Under Document Size, enter new values for the height and width. If desired, choose a new unit of measurement. Note that for Width, the Columns option uses the width and gutter sizes specified in the Units & Rulers preferences.
5. For Resolution, enter a new value. If desired, choose a new unit of measurement, and then click OK.

To return to the original values displayed in the Image Size dialog box, use Alt + click: **Reset**.





Bendix G-15 Computer 1956

Legal Notice

Bay Bytes, Copyright © 2010, is the official newsletter of the Greater Tampa Bay PC User Group, Inc.(GTBPCUG). The information in this newsletter is intended to help our members. It has come from many sources and cannot always be verified. It is recommended that you obtain professional advice from software and hardware distributors, manufacturers, salesmen, or other professionals dealing with the subjects that appear in this newsletter. Unless specifically stated otherwise, the opinions expressed in Bay Bytes articles and columns are those of the individual authors and do not represent an official position of, or endorsement by GTBPCUG.GTBPCUG is not affiliated with any company, vendor or equipment manufacturer. Permission for reproduction of Bay Bytes in whole or in part is hereby granted to other APCUG user groups for internal, non-profit use, provided credit is given to the author, GTBPCUG Bay Bytes along with the copyright notice. Other reproductions require the prior permission of the editor. When published, please send a copy of your newsletter to

editor@gtbpcug.org or mail to P.O.Box 501, Brandon, FL, 33509-0501.