BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.

Newsletter

Issue 9 | September 2012 | 26th Year of People Helping People!

In this Issue

Don't forget to visit our club's site at: http://gtbpcug.org

As well Don Miller's and Darrell Manns' :

http://www.dmanns.org/dmiller/

Can Google Fiber TV compete?

By Marguerite Reardon

Google has blown the pants off the competition when it comes to offering broadband service, but can its new Google Fiber TV service gain traction when the company still lacks popular content?

Google showed off its new Google Fiber TV service at the launch of its new 1Gbps network in Kansas City.

Google Fiber 1Gbps broadband service already looks like it's a step above competitors, but it's unclear how its TV service will stack up against other TV providers' services.

In August Google unveiled its new Google Fiber network that will deliver 1Gbps broadband service to residents in Kansas City.

It also announced a new TV service it calls Google Fiber TV, which will deliver hundreds of channels of programming as well as on demand programming, interactive search capability, and advanced DVR functionality.

In some ways, the all-IP TV delivery network may be superior to existing services from cable operators, satellite TV providers or phone companies offering TV. For instance, the service comes with a DVR that allows users to record up to eight TV programs at once. It also offers 500 hours of video storage capacity on the DVR.

Continued on the next page

Meanwhile, DVRs from competing services top-out at recording up to four programs at once. And many are limited to only two.

Google has also provided innovation in video search capabilities. For example, it allows users to search not just their DVR or the Fiber TV program guide for content, but they can also search across third party online TV services like Netflix.

And because of the high-speed network, Google is able to deliver the very highest quality video in HD on several devices in the same household, including tablets and mobile phones.

But where Google Fiber TV might have trouble stacking up against potential rivals is in providing all the content that users want. Kevin Lo, general manager of Google Access said in a phone interview, that the company will offer TV channels from all the major TV broadcasters, as well as hundreds of "fiber" channels. These so-called fiber channels are many of the same channels from programmers on cable systems.

Still, Google admits it has not signed up every traditional cable programmer. For example, Discovery Channel, CNBC, Comedy Central, and some other big cable names are included in the service. But the company is still missing ESPN, CNN, and HBO.

"It's not a full program line-up yet," Lo admitted. "There is still a small number of programmers not on board yet. But that is coming. Programmers are excited about finding new ways to deliver their content in more compelling and innovative ways."

As other paid TV providers can attest, content is king. And Google must at a minimum offer subscribers the same channels that they can get elsewhere. A lack of content is one of the biggest issues that Google has faced with the slow uptake of its Google TV product. When the company first launched its service, it was seen as a threat to the traditional cable model, and programmers and other content owners would not allow their content to be accessed through the service.

And now Google must compete in the same arena as the cable operators to get customers to sign up for its service. The good news for Google is that the service when taken with the 1Gbps broadband service is almost too good to pass up. The company is charging $120 for the 1Gbps service plus the Google Fiber TV service.

Subscribers also get a $200 Galaxy Nexus 7 tablet for free and the $300 installation fee is being waived right now.

"I've never said this before, but I hope it's you who gets this job."

Passwords and PINs: The worst choices

By David Harley

http://blog.eset.com/2012/06/07/passwords-and-pins-the-worst-choices

After it was discovered that more than six million LinkedIn passwords had been leaked as well as many at Last.fm and eHarmony, no one has stopped talking about password and passcode security.

That's actually a good thing because it's an incredibly important topic that many Internet users don't take seriously.

Case in point, take a look at this new report from IT security consultant Mark Burnett. Self-described as someone who "loves writing about passwords," Burnett has compiled a list of the "top 500 worst (aka most common) passwords" based on a variety of methods he has detailed on his blog.

Here are the top 25, as extracted by antivirus solution provider ESET. Is yours one of them? If so, it's safe to say you should consider changing it to something stronger immediately.

Passwords:

123456	abc123
12345678	mustang
1234	michael
qwerty	shadow
12345	master
dragon	jennifer
pussy	111111
baseball	2000
football	jordan
letmein	superman
monkey	harley
696969	1234567

Guarding against password reset attacks with pen and paper

By Aryeh Goretzky

http://blog.eset.com/2012/06/07/guarding-against-password-reset-attacks-with-pen-and-paper

With the recent announcements of password breaches at LinkedIn, and warnings from Google about state-sponsored attacks on Gmail accounts, it seems like a good idea now to review some password security basics. In this blog post, we're going to take a look at a rather low-tech solution to a decidedly high-tech problem: How to guard against password reset attacks, and where to securely store the answers to your password reset questions.

Even if you use highly secure passwords, it is possible someone might still be able to compromise your account if they were able to gather enough information about you to know—or at least guess—the answers to your password reset questions. Many services use the same questions, *e.g.*, your mother's maiden name, the name of the town you were born in, the name of first pet and so forth. Because similar questions are used over and over again to reset passwords, it can be fairly easy, even somewhat boring, for an attacker who gathers this type of information to use it to gain access to all sorts of accounts one might have, across services ranging from those which are purely social to financial institutions, or even identity theft.

Password Reset Hack Attacks

Sometimes, though, it's even simpler than that: An example of this is former Alaskan governor Sarah Palin, whose personal Yahoo! mail account was compromised via password reset using data about her available from public resources. Of course, most people are not going to have enough biographical data available online to make such an attack easy…. Or do they?

With the rise of social networking has come a kind of blurring of the sorts of personal information it's okay – and safe – to put online. Eager to generate more revenue, social media sites encourage—and in some cases may even require—people to share information about themselves such as birthdays, hometowns, where they went to school and so forth. While this is the sort of information we readily share with friends and family, social media companies request it because it allows for more targeted advertising. The fact that it is the same type of information needed to perform an attack or an impersonation is not something those companies typically tell you about when asking you to fill out your profile, or warn you that profile is not complete.

To date, I cannot recall any criminals going after aggregate personal data *en masse* in order to perform password reset attacks. Data breaches typically provide the password themselves or other information that can be readily used for identify theft, such as birth dates, information about credit cards and, in some cases, even social security identification numbers.

Continued on the next page

Defending Your Passwords

But even if you are not a politician, celebrity or somewhere between the two, you should still take steps to safeguard your privacy and, these days that means some *creativity* is needed when filling out online forms, such when filling in the answers to questions used to reset a password.

One of the largest problems is, of course, deciding exactly what to enter. In the case of birthdates, some web sites, such as online stores, might require you to enter your birth date so they can send you a birthday offer or as the answer to a password reset question. They have no other reason for asking for this information, though, and there's no guarantee they will keep this information secure or use it for other purposes, including selling it to marketing firms. On the other hand, there are plenty of web sites—financial, insurance and government all come to mind —where you may not only need to enter your correct birth date but you may be obligated to give them the correct information.

There's also another issue to consider, both for you and the web site, and that's the issue of ethical behavior. Knowingly providing false data to a web site is something of a gray area, even if there is no legal requirement to do so. How does your obligation to provide a web site with correct information balance with your right to freedom from the theft of that data, let alone the issue of privacy? Measuring these competing—and often contradictory—needs is something everyone has to do for themselves, and we cannot make the decision for you. You will need to decide if breaking this social contract is justified as a matter of practical protection.

If you have made the decision not to enter your actual birth date, than what should you enter? The correct month and day of your birth date, but the wrong year? The correct year, but with January 1st as your date of birth? The date of your favorite holiday? Making the answers to your password reset questions as unique as your passwords is the key to protecting against attacks on them, so using the same answer over and over again is out: That simply provides another widely-disseminated piece of information for a criminal to collect during the data aggregation phase of the attack.

One Low Tech Solution

There is a solution, though, and it is a decidedly low-tech one: Write them down in a small notebook (that is, the kind you write in with a pen or pencil, not a laptop computer). Or, if you are not partial to keeping a little black (or orange) book, a business card or recipe card holder filled with index cards works just as well, too. Store your little "code book" in the area near—but not directly at—the computer, preferably in a location where it is at least out of site. The ubiquitous junk drawer works well for this purpose. Of course, if you use a computer in a shared area, you might want to look at storing your code book in a locked desk drawer, filing cabinet or safe.

Now that we have discussed what to you use your code book for and where to place it for safekeeping, exactly what sort of information should you write in it? I would recommend something along the following lines:

name of web site
username
date you signed up for the service
answer (s) to password reset questions
date of last password change (and/or date of next password change)

For additional security, do not store the actual answers to your password reset questions, but rather mnemonics or clues that will tip you, but not an attacker, to the answers.

Continued on the next page

During the course of writing this blog post, I came across the rather descriptively-named *Personal Internet Address & Password Log Book*, which, as the name implies, is a place to store information about your web site and email accounts. It does, however, contain fields to enter the actual passwords, and not the answers to the questions used to reset those passwords.
Regardless of whether you choose to store password reset questions or the actual passwords, it's important to keep in mind, though, that the physical security of any written-down information in your notebook—whether it be the passwords themselves or just the responses password reset challenges—is paramount: Writing down that information is the equivalent to putting your passport, driver's license, social security card, check book, credit cards and debit cards (and their PINs) all together in one convenient bundle.

If you do not have a place that is physically secure enough to store a password reset notebook in, than you should not be using a notebook for this purposes. Keep in mind that an accident or disaster could result in the notebook being destroyed or unavailable, and plan accordingly. Another thing to keep in mind is that as a tangible, physical object, your password reset notebook is subject to loss. Making a copy of it with a photo-copier and storing that offsite in a secure location like a safe deposit box is far less risky than scanning it and storing the copy on your PC where an attacker can access it.

Password Redux

Choosing good passwords and protecting them, along with the answers to the questions which reset them is vital, but it is only part of the process of staying safe online. Other important components are to keep your operating system and applications up-to-date and running effective security software on your com-puter. Here are some of the recent blog posts and a white paper we have written on the matter:

LinkedIn Privacy: An Easy how-to Guide to Protecting Yourself

Facebook Privacy: An Easy How-to Guide to Protecting Yourself

No chocolates for my passwords please!

Passwords and PINs: the worst choices

Keeping Secrets: Good Password Practice [PDF, 412KB]

In November 2010, ESET North America launched *Cybersecurity Training* to help educate people about the things they need to do beyond running security software to keep themselves safe—something that ESET is the only security vendor to do so far. This online training is free for users of ESET's consumer products. Visit the ESET Cybersecurity Training web site for more information.

If you are looking for even more information about staying safe online, I strongly recommend visiting Securing Our eCity, a non-profit service for protecting yourself, your family and your community from cyberthreats.

The author would like to extend thanks to his fellow password-protector David Harley for assistance in prepar-ing this post.

Aryeh Goretsky, MVP, ZCSE
Distinguished Researcher

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://gtbpcug.org/protect/

More about Internet Threats

Forgotten Passwords

By Leo Notenboom http://ask-leo.com/

In the nine years that I've been answering questions here at Ask Leo!, the single most common topic that I encounter is that of lost or forgotten passwords.
It's been the number one topic since day one.
In the early years, questions relating to lost Hotmail passwords were so overwhelmingly frequent that it became an inside joke among my friends – I was the guy to see about Hotmail passwords.
In the years since, the spectrum has broadened to include whatever system is popular; most recently, it's been Facebook .
Why are so many passwords forgotten? And what lessons can we take away to improve our own security, both online and off?

This isn't about hacked accounts

I've seen the instances of hacked account skyrocket in the past couple of years. Hackers are taking to breaking into email accounts and then using those accounts to send spam to the contacts listed in that account. Not only is a legitimate account more likely to bypass spam filters, but contacts are more likely to open email that came from the account of someone they know.
Hackers will often change the password on the account.
What that means is that when the rightful account holder later tries to login, he cannot. It manifests as a bad password (because it is), and password recovery techniques are the first step to regaining access to the account.
I have several articles covering that scenario already and I'd point you at Email Hacked? 7 Things You Need to do NOW for the steps that you should take if you find yourself in that situation.
That's not what I'm discussing here. This is much more mundane, and yet probably still more common. People forget their own passwords.

Taking it seriously

When I hear the back-story to a forgotten password scenario, there are a couple of frequently reoccurring characteristics:

Continued on the next page

The individual is a relatively new or inexperienced computer user.
They're in a hurry.

In my experience, new users have an underappreciated sense of just how picky computers are about your entering the *exactly correct* password, and perhaps in an effort to make their password secure, they've chosen something obscure and coincidentally difficult to remember exactly. They don't realize just how easy it is to forget the *exact* password that they've chosen.
Newer users are often not online as often as you or I might be, and thus, often aren't even asked for their password more than every day or every week or so. If you're required to enter it correctly every day, it's more quickly committed to memory than if days or weeks go by before you need it again.
More troubling are the folks who are in a hurry. For various reasons, they want an account and they want it **now**. As a result, having to set up a password is more of an annoyance than anything else. Certainly no extra time is spent setting up a *good* password, much less committing it to memory. (More often than not, these are the accounts with passwords like "1234567." They are also more likely to be hacked.)
The common thread is simple: taking security – particularly your password – seriously from the beginning is critical.
Unless, of course, permanently losing access to your account isn't something that you'd consider serious.
"I know of people who've not had to enter their password to login for years."

Your browser remembers so you can forget

Even if you take password security seriously, various conveniences can make it frighteningly easy to forget your password.
I know of people who've not had to enter their password to login for years.
They've allowed the site to "remember" them – forever – or they've allowed their browser to remember their password for them.
The bottom line is that they enter their password exactly once, maybe twice, and then let the browser remember from then on.
Weeks, months, or even years later when for some reason or another they need to login elsewhere, they have no idea what their password is. They've set up their life so that they've simply never had to type it in after setting it up to begin with.
The sad news about most browser password stores is that they're often only lightly secured themselves and are accessible not only to individuals with access to your machine, but to malware as well. I avoid them.

Passwords one through one hundred

The classic "rules" for password are frustrating in that they seem to be crafted specifically to make passwords impossible to remember:
Passwords should be at least 12 characters long1.

- Use a mixture of character case and type (letters, numbers, special characters).
- Don't use words or names.

Don't use the same password on more than one site.

Yikes! If you're only allowed to use passwords like "P5S0Dk@!i2Yd", "#zJCahT0kAA3" and "4Jy% zsX6H9!^", *and* you're not allowed to re-use them, then it's no wonder we can't remember them all!
Even when choosing something slightly less secure than those rules, the best of us would fail miserably without help of some sort.

Continued on the next page

Technique 1: The algorithm

One approach to generating memorable (or "remember-able") passwords is to use an algorithm or a set of rules to create *all* your passwords. For example:

- Begin with a memorable quote (or phrase or song lyric or ...)
- Use the first (or last or second or ...) character from each word in that quote

Add into the middle (or beginning or end or ...) the first and last characters of the domain that you're setting a password for.

So, let's say I use the first 10 words of The Gettysburg Address:
Four score and seven years ago, our fathers brought forth

Now, I'll use the first letter of each word:
Fsasyaofbf

Let's say I'm setting up a new Hotmail account, so I might use the first and last letters of the domain (hotmail.com) and I'll insert them into the middle:
Fsasyhlaofbf

Given that you always remember your own algorithm or password generating rules and always remember the phase or song lyric or quote you start with, then regenerating almost any password you created using those rules is a snap.

Technique 2: The pass phrase

Longer passwords are better. In fact, the longer the password, the more acceptable it is to break some of the other "rules" associated with passwords.
Enter the pass *phrase* – a sequence of words (yes, dictionary words) that you can remember that is significantly longer than your old eight- or 12-character password.
For example, the pass*phrase* "correct horse battery staple" would be considered a better password[2] than, for example, "P5S0Dk@!i2Yd" by virtue of it being significantly longer – 28 characters as compared to 12.
A passphrase doesn't have to be "weird" or nonsensical – although I suppose it helps – a good, lengthy passphrase can be anything that you would easily remember.
No problems making it unique to each site, either. Modifying your passphrase in a site-specific way, for example "correct horse battery hotmail," works great.
The frustrating downside to passphrases is that they don't work everywhere. Many sites, for inexplicable reasons in today's world, limit the length of passwords to something silly like 16 characters. (Or worse, only *pay attention* to the first N characters.) Often, they don't accept spaces. These limitations often prevent us from using secure passphrases for some logins, requiring us to fall back to more traditional and often less secure techniques.

Technique 3: Admit you need help

I don't know my online banking password.
It's not that I forgot it; I never bothered to even try to remember it. And it's quite secure and obscure.
So how do I get in?
I admitted defeat when it comes to my memory long ago.[3] I use a password storage tool: Lastpass.
The concept here is simple: remembering a single, strong password to unlock the vault, the tool contains a database of all my other logins and passwords and works within my web browser to enter them automatically as needed, or on demand.
Lastpass remembers so I don't have to.

Continued on the next page

Tools like Lastpass are significantly more secure than allowing your browser to just remember your passwords for you. Lastpass was built for security from the ground up. Without your master password, your vault is inaccessible and Lastpass can be configured to require you to supply your master password every time; after your computer's been idle for certain amount of time or after your browser's been closed and re-opened. (Lastpass specifically also supports two-factor authentication for additional security, particularly useful if you travel.)

Take it seriously from the start

The real bottom line to not becoming "one of those people" is to take your account security and password seriously from the moment you open your account.

- Select a technique that you *know* will allow you to remember or regenerate it as needed.
- Choose a strong password – the longer the better.
- Make sure to properly set up (and remember and keep current) additional account security options such as mobile numbers, secret questions, alternate email addresses and more.

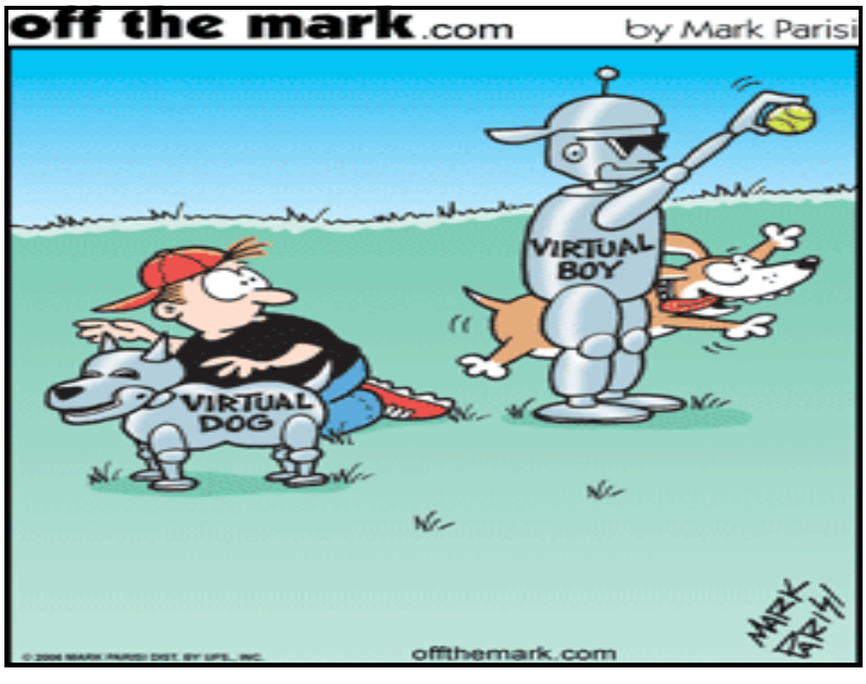
If you want to use technology to remember things for you, opt for a tool like LastPass specifically designed for this job.

Above all, take your time and do it right from the start.
Trust me, a little extra time and thought now will help avoid a lot of pain in the future.

1. The old rule of eight that many of us "grew up" with is no longer secure. Passwords these days should be 12 characters or longer.

2. OK, this *specific* example is an incredibly *poor* passphrase as it's been used frequently as an example of a very good passphase. So don't use it. Use your own set of words to make a passphrase.

3. My wife would agree to the defeat, but not to my ability to consistently admit it.



How to Detect a Rootkit

By Bob Rankin http://askbobrankin.com

A rootkit is a type of malware package that is extremely difficult to detect and eradicate. That's because a rootkit actively hides itself from standard operating system tools like Task Manager and Windows Explorer. Worse, a rootkit often disables anti-malware programs found on the infected system. The rootkit may also block access to Web sites that offer help with rootkit elimination, or even prevent your browser from opening at all.

Since you can't see a rootkit, you can only infer the possibility of one from otherwise inexplicable abnormal behavior on your system. Some symptoms of potential rootkit infection include:

A spate of system crashes (the Blue Screen of Death) on a system that previously ran trouble-free.

Random system slowdowns indicating that something invisible is consuming network or system resources. Task Manager's Performance or Networking tabs may indicate an unusually high level of CPU or network activity.

Erratic behavior of input and pointing devices, i.e., mouse freezes, keyboard does not respond.

Anti-malware program does not start with system reboot.

You can't access certain Web sites, particularly sites devoted to security issues, or cannot open Web browser at all.

Unusual increase in network traffic; something is using your Internet connection without your knowledge.

Rootkit Detection and Removal Tools

If you've already done a through scan for malware and viruses, it's time to try a more specialized tool. Some tools that can help locate rootkits on a system include Microsoft Rootkit Revealer, Tizer Rootkit Razor, and IceSword. But these tools are not one-click solutions to rootkit problems. It takes pretty advanced technical skills to interpret their findings, and even more to actually do something about a rootkit.

Rootkit removal utilities for non-technical computer users are relatively rare, probably because rootkits themselves are rare. F-Secure Blacklight detects objects that are hidden from users and security tools, and offers the option to remove them. Trend Micro's RootkitBuster is a standalone rootkit eradicator from a trusted name in anti-malware products. Sophos Anti-Rootkit is another free rootkit detection and removal tool.

It's best to run multiple rootkit scanners on a system you suspect is infected. No anti-malware program catches everything. Even if all of the scans turn up negative for rootkits, there is still a chance that your computer is infected. I've been saving the worst news for last.

The only way to be 100 per cent sure you have eliminated a rootkit is to wipe your hard drive completely and re-install everything from trusted media (like a CD or DVD). And by "wipe," I don't mean simply reformatting the drive. You need to delete the partition(s), shut down the computer to kill any malware that may lurk in RAM, and re-boot from your Windows CD. Then start all over with creating partition(s) and installing the OS, application software, etc. If that sounds daunting, see my articles Reformat Hard Drive Under XP and Reformat Windows 7 Hard Drive for some help with the process. Preventing rootkits from installing themselves on your computer is the best strategy, obviously. Use the Internet only from a limited-user account, not from an administrator account. Be careful what you download and click on, and keep anti-malware software up to date

What is Google Redirect?

By Bob Rankin http://askbobrankin.com

If you click on a link in a Google search result and get taken to a totally unexpected Web page, you may well have a malware problem. Google Redirect Malware is malicious software that redirects all of your Google search clicks to pages that serve up ads, more malware, phony anti-malware programs, etc. It can be extremely frustrating because you can't search Google for a solution. It's also very dangerous because it usually does much more bad than simply messing up your Google searches.

Google Redirect distracts the user with bizarre search result redirections, while in the background it may be collecting passwords and other sensitive data, using your computer to send spam, and letting remote bad guys do whatever they wish with your system.

Despite the name, Google Redirect malware is not a bug in any Google service. It's a malware infection that resides on your computer, and was created by cybercriminals. It doesn't matter which Web browser you use; all of your Google searches will be redirected. The only solution is to track down and eliminate the malware on your hard drive.
Google Redirect spreads when users are tricked into downloading malicious programs or clicking unsafe links in email. And unfortunately, Google Redirect is no ordinary malware. Some anti-malware programs miss it, because Google Redirect is a rootkit package that hides among your system files. For details about rootkits and why they are so hard to remove, see my article,I Think I have a Rootkit

Eradicating the Google Redirect Malware

Defeating the Google Redirect virus usually requires specialized rootkit-removal software. You may want to download some of these toolkits now, and store them on secure media such as a USB flash drive or a CD. After all, when you need them you won't be able to use Google to find them!

Kaspersky Labs' TDSSKiller detects and removes a variety of stubborn malware, including the TDSS rootkit that underpins many variants of Google Redirect. It's GUI is simple enough for non-technical users to follow safely. Just unzip the download file, run the program, and scan for malware. It works on 32-bit and 64-bit Windows systems, and can be used in Normal or Safe mode.

Norton Power Eraser can also detect and remove rootkits like Google Redirect. It aggressively scans for rootkits and tags suspect files for review by the user. It should be used with caution; eradicating the wrong system file can lock up your computer. Power Eraser runs on Windows XP, Vista, and Windows 7, and can be used in Normal or Safe mode.

I strongly advise you to create a System Restore Point before running either of these programs. That way, if you eradicate the wrong file(s), you can restore your system to its previous state and try again. If you're not familiar with System Restore, see my article Time Travel with System Restore to learn how it works.

Have you been affected by the Google Redirect malware? Tell me if you found another way to solve the problem.

The lighter side

http://www.worldstart.com/memory-vs-storage-whats-the-difference/

Memory vs. Storage: What's the Difference?

I've Always Wanted To Know:
What is the difference between memory and storage when it comes to computers? Why are there two different types?

Answer:
When it comes to computers there are two terms people are often confused about: memory and storage. The confusing thing is depending on the manufacturer or advertisement the words can be switched or replaced with other ones like hard drive, ram, disk, hdd, random access and a host of other terms. So what does each do and why does a computer need both?

RAM

Synonyms: Memory, Random Access Memory, short term memory, DDR memory, DDR2 memory, DDR3 memory

Use: RAM is used for temporary storage of data programs are accessing and changing. This data is loaded off a storage device or created by the program and stored in the RAM until no longer needed or the program is closed. RAM requires a constant power source to hold information and will clear the information if the power is removed. RAM is many times faster then conventional storage devices and as such is perfect for working with while a program is running.

Words you may find around RAM:
DDR, DDR2, DDR3, GDDR3, GDDR5, LPDDR, LPDDR2, LPDDR3, ECC

Continued on the next page

Hard Drive:

Synonyms:
Disk Drive, Storage, HDD, Permanent Storage, SSD
Use: A hard drive is used to store information for long term purposes and retains the data stored on it when the power is removed from the hard drive. Hard drives often have much larger capacities than RAM chips and cost less per gigabyte of storage. Hard drives are used as long term storage instead of temporary storage due to the slow transfer times (compared to RAM.) Hard drives typically refer to mechanical drives which use magnetic storage but some newer drive types use flash memory which retains information when power is removed. These flash based storage devices can be referred to as SSD or solid state drives as they lack moving parts.

Words you may find around hard drive:
HDD, 7200 RPM, 5400 RPM, SSD, Raid, Disk configuration, SATA, IDE, SAS

So what's a good amount and type of each to look for in a new computer (as of August 2012)?
8 GB (Gigabytes) of RAM (or more) and 500GB (or more) of hard drive space is as low as you want to go on a new desktop or laptop. If you want really good performance make sure your ram is the DDR3-1600 (or higher) variety and the hard drive is either a SSD as primary drive and a regular hard drive for storage or at least a 7200 RPM regular hard drive if only one drive is included.

Some of the material appearing in this Issue was sent to the editor by other members of the GTBPCUG. Thank you.