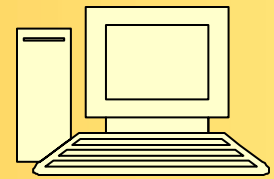# Bay Bytes

Greater Tampa Bay Personal Computer User Group, Inc.

Newsletter

Issue 3   **March 2013**   27th Year of People Helping People!

GTBPCUG

March 2013

Newsletter

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/

Most XP machines are getting up in age and could give up at any time. Most of them still do have a Floppy A: Drive to boot from and this tip below might come in handy. Ed.

How Do I Make a Windows XP Bootup Disk?

What happens if you are unable to start your computer because the Operating System (OS) could not be loaded? This could happen when any file used for the booting process becomes corrupt or lost, or if your system has been affected by a virus.

You need a set of clean files that will allow you to load the OS and access the file system and services in case your PC is unable to boot. Keeping a backup of the files critical to this functionality on a Bootup disk is good practice.

Let us see what exactly happens when you turn on your computer - the BIOS is loaded first. Normally, the BIOS runs some tests on the system hardware at startup, after which it locates a bootable device on your computer (Floppy, CD-ROM, Hard disk) and the Master Boot Record (MBR) is loaded into the memory. The MBR locates the active partition and loads the boot sector into the memory. The boot sector has the code to start the bootstrap loader which then loads the OS (Windows, Linux, Unix, MacOS) into the memory.

In case of Windows XP, the bootstrap loader is called Ntldr. The bootstrap loader must be located in the active partition, in the root folder. In addition to this file, Windows XP also requires Ntdetect.com, boot.ini, bootsect.dos (for dual boot) and Ntbootdd.sys (needed if you plan to use SCSI devices) to be available in the same folder, on the active partition.

Ntldr uses Ntdetect.com, boot.ini, and bootsect.dos to let you choose the operating system that is to be loaded. Once Windows XP is chosen from the boot menu, Ntldr runs Ntoskrnl.exe which in turn launches Winlogon and Lsass, which then displays the welcome screen and allows you to log on.

Any Bootup floppy you create must be done on a system that has Windows XP already working on it and is free of viruses. Insert a blank floppy in the floppy drive; format it by right clicking on the floppy icon.

Once you have a formatted virus-free floppy in a virus-free system, copy Ntldr, Ntdetect.com, and the boot.ini files onto the floppy. You can either copy these files from the Windows CD-ROM or from your computer. As an added measure, the edit program available in windows could be copied on to the Bootup disk so that you can use it to edit boot.ini if necessary.

For all you XP users. From Terry Stockdale

Safely eject the USB Drive when the Icon is not displayed

Subscriber David wrote to ask about a USB flash drive problem he has occasionally:

I often find that the tray icon in XP for my USB devices disappears in the middle of a session. I cannot figure out how to safely eject a USB device when this happens.

I tried turning off the feature of the computer getting rid of unused icons but that did not seem to help.

Even so, if I cannot figure out an alternative to clicking on this icon, taking it away because it has not been accessed is problematic. So this is two questions...

The first is how to keep that icon from disappearing and the second is how to safely eject without using the icon.

As to David's first question — how to keep the icon (presumably the Safely Eject Hardware icon) from disappearing, I don't know. I don't recall having this problem when I used Windows XP.

However, perhaps the reason I don't remember it is that I know how to "Safely Remove Hardware" when the corresponding icon is not available in the Windows Status bar (now called the Notifications Area).

The first step is to find the drive in Windows. Open **My Computer** or open **Windows Explorer** (in Windows XP, right-click on the Start button and click Explore; in Windows 7, right-click on the Windows Orb and select Open Windows Explorer).

Find the USB drive in **My Computer** or **Windows Explorer**. Then, right-click on the icon for the USB drive. One of the options is Eject, which is what you want to do.

By the way, if you have any program or window open that is using, or otherwise has open, a file or folder on that drive, you will not be able to eject it (or use the Safely Remove Hardware icon, even if it was visible).

_____

"I no longer sell hot dogs from here. All my vending is now done online."

Hubs, switches, and routers are all computer networking devices with varying capabilities. Unfortunately, the terms are also often misused

# What's the difference between a hub, a switch, and a router?

In a word, intelligence.

Hubs, switches, and routers are all devices that let you connect one or more computers to other computers, networked devices, or even other networks. Each has two or more connectors called ports into which you plug in the cables to make the connection. Varying degrees of magic happen inside the device and therein lies the difference. I often see the terms misused, so let's clarify what each one really means.
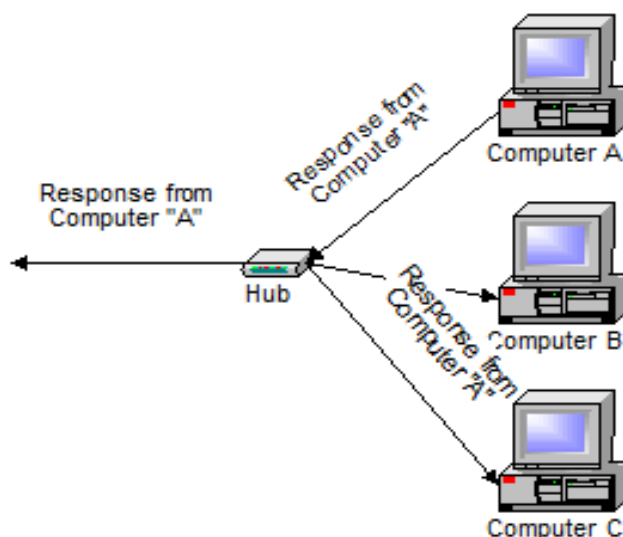
Hubs:

A hub is typically the least expensive, least intelligent, and least complicated of the three. Its job is very simple - anything that comes in one port is sent out to the others.

That's it. If a message† comes in for computer "A", that message is sent out all the other ports, regardless of which one computer "A" is on:
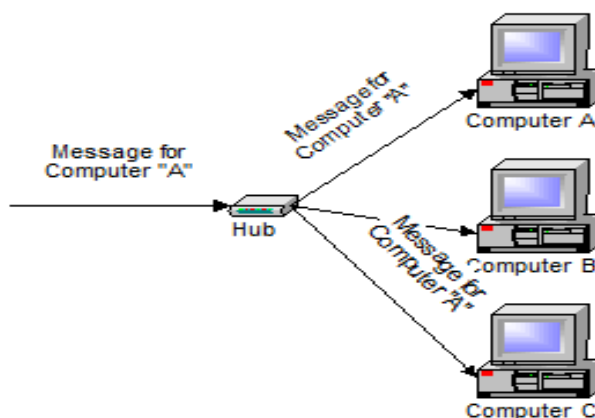
And when computer "A" responds, its response also goes out to every other port on the hub:

Every computer connected to the hub "sees" everything that every other computer on the hub sees. The computers themselves decide if they are the targeted recipient of the message and when a message should be paid attention to or not.

The hub itself is blissfully ignorant of the data being transmitted. For years, simple hubs have been quick and easy ways to connect computers in small networks.
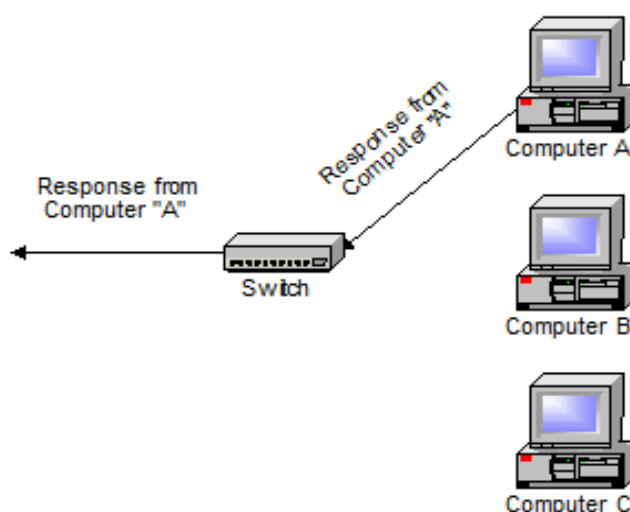
Switches:
A switch does essentially what a hub does, but more efficiently. By paying attention to the traffic that comes across it, it can "learn" where particular addresses are.

Initially, a switch knows nothing and simply sends on incoming messages to all ports:
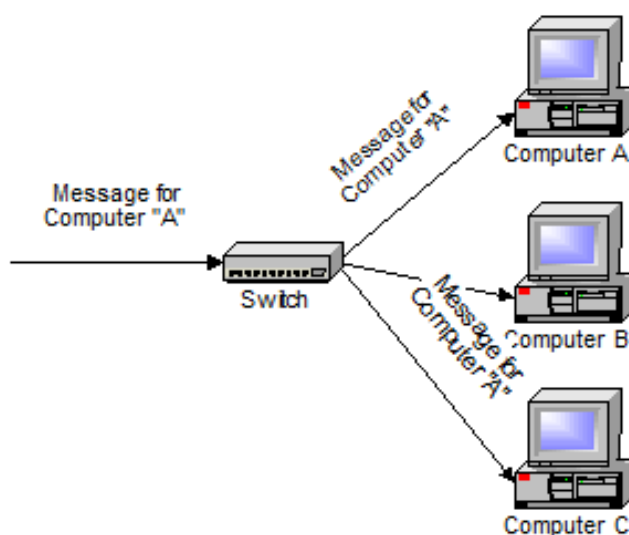
Even accepting that first message, however, the switch has learned something - it knows on which connection the sender of the message is located. Thus, when machine "A" responds to the message, the switches only need to send that message out to the one connection:

In addition to sending the response through to the originator, the switch has now learned something else - it now knows on which connection machine "A" is located.

That means that subsequent messages destined for machine "A" need only be sent to that one port:
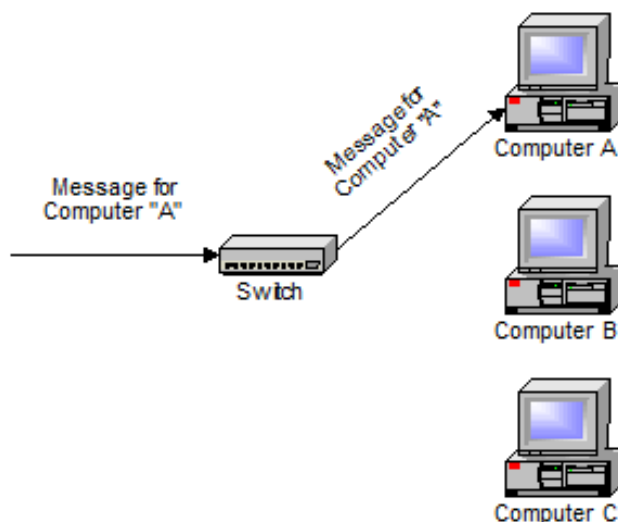
Switches learn the location of the devices that they are connected to almost instantaneously. The net result is that most network traffic only goes where it needs to rather than to every port. On busy networks, this can make the network *significantly* faster.
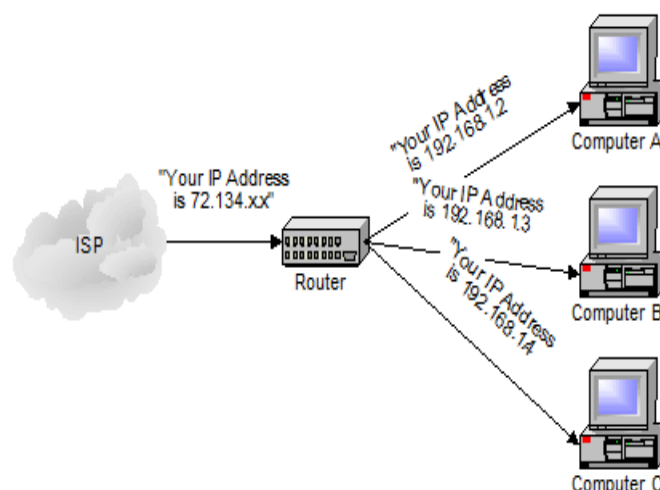
Routers:
A router is the smartest and most complicated of the bunch. Routers come in all shapes and sizes - from the small, four-port broadband routers that are very popular right now to the large industrial strength devices that drive the internet itself.

A simple way to think of a router is as a computer that can be programmed to understand, possibly manipulate, and route the data that it's being asked to handle. Many routers today are, in fact, little computers dedicated to the task of routing network traffic.

As far as simple traffic routing is concerned, a router operates exactly as a switch, learning the location of the computers on its connections and routing traffic only to those computers.

Consumer grade routers perform at minimum two additional and important tasks: DHCP and NAT.

DHCP - Dynamic Host Configuration Protocol - is the way dynamic IP addresses are assigned. A device asks for an IP address to be assigned to it from "upstream" and a DHCP server responds with an IP address assignment. A router connected to your ISP-provided internet connection will typically ask your ISP's server for an IP address; this will be your IP address on the internet. Your local computers, on the other hand, will ask the router for an IP address and these addresses are local to your network.

NAT - Network Address Translation - is the way that the router *translates* the IP addresses of packets that cross the internet/local network boundary. When computer "A" sends a packet out, the IP address that it's "from" is that of computer "A" - 192.168.1.2 in the example above. When the router passes that on to the internet, it replaces the local IP address with the internet IP address assigned by the ISP. It also keeps track, so that if a response comes back from somewhere on the internet, the router knows to do the translation in reverse - replace the internet IP address with the local IP address for machine "A" and then send that response packet on to machine "A".
A side effect of NAT is that machines on the internet cannot initiate communications to local machines - they can only respond to communications initiated by those local machines.
The net effect is that the router then also acts as a firewall:
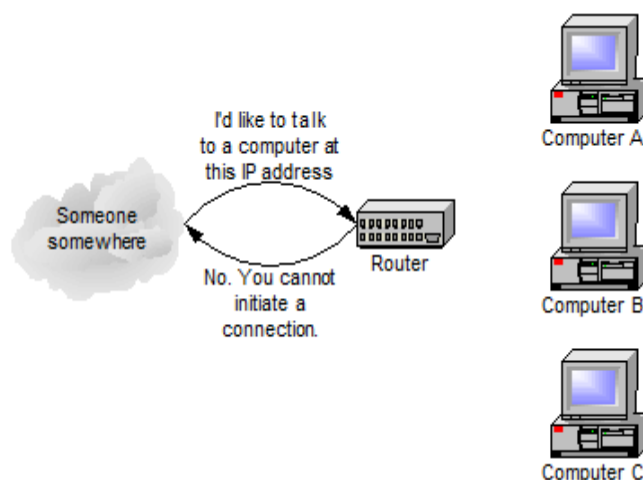
What that means is that malware that might spread by trying to independently connect to your computer over the network cannot.
All routers include some kind of user interface for configuring how the router will treat traffic.
The really large routers include the equivalent of a full-blown programming language to describe how they should operate as well as the ability to communicate with other routers to describe or determine the best way to get network traffic from point A to point B.

A note about speed

A quick note on one other thing that you'll often see mentioned with these devices and that's network speed. Most devices now are capable of both 10mpps (10 mega-bits, or million bits, per second) as well as 100mbps and will automatically detect the speed.

More and more devices are now capable of handling 1000mbps or a billion bits per second (1gpbs). Similarly, many devices are now also wireless transmitters that simply act like additional ports on the device.

Comments & updates at: What's the difference between a hub, a switch, and a router?

You may also be interested in:

- How do I secure my router? Your router is your first line of defense against malicious attacks from the internet. But is your router secure? I'll review the important settings.

- How should I set up my home network? Once you add a second computer to you're faced with setting up a network, at least to share the internet connection. Here are some general guidelines.

- What kind of router do I need? A router is a router is ... actually, there are several different kinds of routers that are used in different situations. I'll review the most common.

- What's the difference between a router, a wireless router and a wireless access point? Unfortunately, terminology has become quite confused around routers and access points, I'll describe each, how they relate, and why differences matter.

_____

Dick

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…   *and other Malware, Spam and Users beware*

Is The FBI Holding Your Computer for Ransom?   http://askbobrankin.com

A concerned reader asks: *'A popup on my screen says an FBI Online Agent has detected illegal activity on my computer, and is demanding $200 to unlock my computer. What should I do?'*

Here's what you need to know about this so-called FBI Virus...
But you're innocent, right? (Let's hope so...) Well, this scam actually did scare one child porn consumer into turning himself in to the FBI. But that's not you, and the government doesn't operate this way, anyhow. Of course, the U.S. Federal Bureau of Investigation has nothing to do with this scam. (If the government wants more money, they can just raise your taxes.)
But that's not the only issue; you can't do anything with your computer until the "fine" is paid. Many people panic and pay the "fine" just to make the problem go away. But it doesn't go away; it only gets worse. Once you've paid, more demands for payment arrive. Don't bother going to the Add/Remove Programs icon in your Control Panel. The Reveton/FBI malware doesn't contain the usual "uninstall" code, because it wasn't intended to be removable.
The FBI Virus is a "drive-by" malware; it's downloaded secretly to any browser that visits an infected Web site. Many of these rogue sites are porn or "warez" related, but any site could host the Reveton/FBI virus code. So don't assume that "responsible surfing" will keep you safe.
Your best line of defense is up-to-date, real-time anti-malware software. Free programs I've recommended in the past will greatly reduce the chances that you will catch the Reveton infection.

Tools to Remove the FBI Online Agent Virus
Removing Reveton/FBI is difficult; some experts recommend letting a security professional do it. If you want to remove Reveton yourself, you can restart in Safe Mode and fiddle with the Windows registry. (I don't recommend this method, but you can Google for those instructions.)
The best method is to reboot your computer from a CD or USB drive that contains appropriate anti-malware software. If you don't already have such a rescue disc or flash drive, you'll have to download it and install it on removable media from a clean computer. I recommend the AVG Rescue CD for this purpose. Booting up from the rescue disk will bypass the virus, and commence a scan and removal operation to return your computer to normal.
Norton Power Eraser is one free tool that can remove Reveton and other stubborn malware. The free or paid versions of MalwareBytes AntiMalware can also do the job.

HitmanPro is designed for removing ransomware like Reveton, rootkits, and other malware that interferes with the installation or use of regular antimalware products. It comes with a 30-day free trial and costs $20 to register for permanent protection. Never pay a "fine" if you are struck by the FBI Virus or any other malware that demands ransom. Rest assured the FBI would have no trouble finding your front door if they really wanted to discuss a criminal matter with you. If you pay the ransom demanded, you're only lining the pockets of cyber-criminals and setting yourself up for further grief.

Should You Defrag an SSD?

With a lot of more modern computers using SSD's (Solid State Hard Drives), one question I often get asked is if you need to defragment a SSD. That's a good question because up until now, pretty much everyone has defragged their computer at least once.

So why do we defragment a hard drive in the first place? Well, I won't go into super detail here since you can read about it online, but basically it's because spinning hard drives taker longer to read data that is "fragmented" or stored in multiple locations on the hard disk. Since spinning hard drives read and write data sequentially, it will take longer for the hard drive to read a file if parts of the file are located on different parts of the disk as compared to being located altogether in one unit/space.

So defragmenting a normal spinning hard drive can be useful depending on the size of your drive, the number of files you have stored and the size of those files. Now the question becomes is defragmenting useful if the hard drive has no physical moving parts?

Well, the answer to that question is pretty easy once you understand the difference between an SSD and a HDD. An SSD is basically non-volatile flash memory, which you are probably used to using in your digital camera, etc. An SSD is fast because it randomly accesses memory instead of sequentially like an HDD. SSD's are great, but there is one huge caveat that most hard drive manufacturer's never mention about SSDs and that's their lifespan.

Because of the way they are built, an SSD wears down every time they are written accessed. If you have read reviews of SSDs before, you have probably read about how an SSD will get slower if you benchmark it after completely filling the drive and then erasing it. With a HDD, you would never have that problem. Most people mistakenly think SSDs are safer than HDDs because they have no moving parts. This is not true. Flash memory has a very finite lifespan and the more it is used, the more quickly it will fail.

So back to the question of defragmenting. When you defrag a hard drive, especially a SSD, it will end up causing tons of small write accesses, which will reduce the lifespan of the hard drive. And since data is not being read sequentially, it doesn't matter if the file is stored in a hundred different places, the performance will remain the same.

So, no, you should not defrag an SSD. And performing one will actually reduce the life of your drive. All of the SSD manufacturer's know of this problem and they have come up with an optimization technique with the use of the TRIM command.

Currently, with HDDs and SSDs, if you delete some data on the hard drive, the operating system does not actually remove the content from the disk, it just deletes the pointer to the address and therefore "deletes" the data. That's probably why you're heard of secure delete or government security file deletion, which actually overwrites the deleted data with gibberish so no one can use advanced tools to read data later on.

This issue of data not actually being deleted is what causes the lifespan of SSDs to be reduced. If the drive knew which areas of memory didn't contain any important data, it could simply re-use it for new data. The TRIM command is supported by the latest SSDs and will optimize the hard drive so that it reduces the number of writes/deletions and therefore extends the life of your SSD significantly. If you're in the market to buy an SSD, make your choice very carefully. You want a hard drive that supports the TRIM command. Some of these include:

- Intel X25-M and X18-M G2 G2
- Indilinx Barefoot
- SandForce SF1200 / SF1500 Force
- Samsung RBB
- Samsung 470

There are a lot of other SSDs that support the TRIM command, but you have to check with the manufacturer. Note that Windows 7 natively supports the TRIM command for hard drives that support it, so you don't have to do anything. Older versions of Windows do not support the TRIM command. In the case of Windows XP and Vista, the OS cannot even tell the difference between an SSD and a HDD, so it's best to turn off the Disk Defragmenter.

You can also use third party programs that support TRIM to run on systems not running Windows 7. If you don't believe everything I've said, then you can check out this post from a more reliable source that details exactly why it's not a good idea to defrag a SSD:

http://www.oo-software.com/en/docs/whitepaper/ood_ssd.pdf

Problem Computer, and how Guru Gary fixed it   **By Emi Evans**

I first began to suspect I had a computer problem when the Internet Explorer icon disappeared from my task bar, and I had to click on the IE icon on my desk top to access the internet. Normally, on my computer, the MSN homepage appears. This time MSN appeared with an ominous popup, warning me that my computer was about to crash, and instructed me to click the box on the pop-up to fix the problem.

OH OH! Red flags go off in my brain. I don't think I'll do that!

I tried other clicks outside the pop-up to try to get rid of it, and it did disappear, only to reappear with a vengeance. I tried to remove the page from my desktop, but my computer wouldn't acknowledge any command.
OK, I'll reboot with the Ctrl+Alt+Delete command.

This worked. COOL! Tried email. This worked fine.

Tried accessing the internet through Firefox. This worked fine too.

Tried accessing the internet through Google....then Bing. Both worked fine.

Now I'm thinking that IE is corrupted.

I rebooted with Ctrl+Alt+Delete again, then ran C-Cleaner, MalwareBytes, and SuperAntiSpyware and found multiple problems.
Now I'm REALLY bummed out because this stuff never happens to my computer. OH OH!
I cleaned out the problems, then I tried to access IE through Google to restore the icon on my task bar again. The pop-up with the crash warning reappeared.

I called Gary [at CALLGARY-1-800] and explained my problem.
He sent me a filehippo.com download and told me to be very careful when using this tool.

I had never gone into my computer registry before, and when I got there I had no idea what I was looking at. So I called Gary and asked him to look at my computer and walk me through the clean-up. We used the Microsoft program REGEDIT to find and delete two problems in the registry that hi-jacked my computer. Watch for 'Whitesmoke' and 'Conduit'. Once those bad boys were removed, I no longer had threatening, hard-to-remove popups. I can probably/maybe/hopefully clean up registry problems alone next time...(if I feel brave enough), I will heed Gary's advice: "Don't remove some-thing if you think you need it."

I remember various club members advising us to always uncheck boxes when installing programs, but I can't remember any recent downloads, nor the words mentioned above. Who cares how the problem arrived. The flashing threat is gone.

Thanks, Gary! You're a great teacher.

Finally, a member took time out to put in print what happened to her PC. Thank you Emi.
Hopefully other members will follow to do so.
The Editor.

The lighter side...

By Rob Zanicchi

More than 20 years ago, [Bill Gates](#) publicly predicted what may have seemed obvious to several of Silicon Valley's finest -- email was going to be huge. While being interviewed on *NBC's Today Show* recently, the Microsoft co-founder was shown a portion of an interview he did back in May of 1992 where he accurately detailed how the adoption of email was soon to explode. Then 36, the multibillionaire describes how the desktop computer would gain momentum and mold an essential form of communication. In fact, he was surprised that it wasn't "happening a little faster."

Jump ahead 20 years to the present, and email has obviously become an intricate part of modern society, with widespread use across plenty more devices, too. From [Google's Gmail](#) to Microsoft's own [Outlook](#), electronic mail paved the way for dozens of webmail providers and endless amounts of software to help us all stay in touch from our devices. These days, Microsoft is still a strong force in the PC arena, though it's essentially been playing catch up in the tablet and mobile arenas -- its fledgling iPad alternative, the [Surface tablet](#), and Windows Phone 8 offerings haven't really trumped the [competition](#) like Redmond once had years ago.

As for Bill Gates? The future of Microsoft won't totally be led by the innovator, as he removed himself from the day-to-day duties of the company several years ago to focus on [philanthropy](#). Still, if you want to experience some more of his insight on technology and education, you'll have to catch him at one of his many speaking events -- [Bill Gates' TED Talk](#) ([Technology, Entertainment & Design](#)) is scheduled to air on PBS on April 16th.

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