Training Young Troubleshooters

Computer Hardware, Software, and Troubleshooting Curriculum

Developed by Matthew Hagaman

This unit consists of four different modules, each of which may be used individually or in conjunction with the other modules. Modules might be used in whole or piecemeal, depending on the needs of your students and the constraints afforded by time and materials.

Reading Guide

Most activities consist of three or more sections:

An instructor's introduction, intended to provide any needed background and establish the goals and expectations related to the activities.

A list of materials. A number or ratio of needed materials is provided only as necessary: most often material requirements are flexible and can be adjusted to meet the needs of any instructional environment.

Activity instructions, written in a direct-to-student format: in many cases, the lesson would make sense if the activity instructions were read to students. Activities are provided in this format only to ease the use of lesson plans in the classroom; lessons are not necessarily intended to be read word-for-word. This format is broken between sections of a multi-part lesson to differentiate between student and teacher instructions. Times are VERY rough estimates, and will need to be tweaked to match your students and objectives.

Scoring information is only provided if I have used that lesson in my classroom and graded it for correctness / completeness rather than participation credit. Oftentimes allowing students to gain experience is much more valuable than proving mastery – these lessons generally do not include enough practice for students to reach mastery.

Throughout the activities, hints directly related to troubleshooting are highlighted.

Special preparation instructions / cautions are boxed in and printed in dark red text.

This curriculum is a work in progress.

Any updates will be posted to my website at http://mthagaman.com/?tyt. Please send me an e-mail if you have any suggested improvements: matthew [at] mthagaman.com.

Module 1: Computer Hardware

The computer hardware module gives students a hands-on orientation to the parts of a computer, expanding their understanding beyond the keyboard and mouse and into the "magic box" that is the computer.

Activity 1-1: Computers and Their Components

While I have had students dive into demanufacturing a computer without knowing its parts, our experience has been richer when students have gone into the project with some background information. In particular, it has been useful for students to understand the components they are touching as they go about that activity.

Whether or not you give students the opportunity to break a computer down into its parts, it is useful for students to gain a basic understanding of computer parts in order to make later activities more meaningful.

Materials

- Copies of or student access to *Computers and Their Components* Reading (page 28)
- A collection of computer hardware components, including:
  - DVD drive
  - Hard drive
  - Heat sink
  - Memory / RAM
  - Motherboard
  - Network card and/or modem
  - Power supply unit
  - Processor / CPU
  - Sound card
  - Video card

Activity (20m)

Today we are going to read about the different parts that make up a complete computer system. While these parts are easy to find in a computer tower, they are part of nearly every electronic device we use today, including your phone or tablet. Gaining an understanding of the role these parts play in a computer system will help us as we explore our unit.

As we go through the two-page reading together, I invite students to share what they know about them. Oftentimes students will be able to identify brands of components such as AMD or Intel, which brings additional background information into the discussion and allows students to make richer connections.

Activity 1-2: Demanufacturing

In an age of mobile computing, it is sometimes difficult to inspect the hardware inside a computer system. With that being said, it has not become any less important: mobile devices still utilize processors and random access memory, and blown capacitors can cripple any system.

If you have access to desktop or tower computer and a variety of tools, students always enjoy the process of dismantling a computer. While they do so, they can learn about the components of the computer as well as how each part connects to the rest. They can learn far more from touching each component as part of a working configuration than they will from a mere reading.

Materials

- Complete computer systems, destined for recycling (1 per pair of students)
  You might be able to get computer towers from your IT department, from a nearby university, or a local recycler. As long as you emphasize that students will de- and re-manufacture the equipment, and that you can return the equipment in the same configuration, recyclers are usually happy to help.
- A variety of #1 and #2 Phillips screwdrivers and 1/4 and 3/16 slotted screwdrivers (1-2 drivers per student or at least one of each type for every two groups). Torx 10 and 15 drivers may be required occasionally.
- A pair of wire cutters for teacher use (needed to get through zip ties...cutting wires is not recommended!)
- A way of labeling students' computers so they can return to the same system every day

Activity (60 minutes)

What does demanufacturing mean? *To disassemble an electronic device into its original components.*

Today you will be demanufacturing a computer system in order to learn all of its parts. Before you begin, make sure your computer is unplugged and that you have equalized any static electrical potential by touching the metal of the computer case. (Static electricity could potentially fry your computer!) As you break it down into components, you will want to keep track of its source; you might use blank paper to draw a map of where each item came from, including screws of different sizes.

If they are available, use plastic “quick release” features rather than removing screws. When you do need to remove a screw, apply more pressure down on the screw than you do turning it so you can avoid stripping screws. Be careful to remove only the necessary screws: the screws that are part of a component (for example, the power supply) do not always need to be removed in order to loosen the whole component.

When your demanufacturing is complete, you should have removed all of the named components from our reading and internal cables should be unplugged from both ends.

Once you have disassembled your computer, you will want to spend some time reviewing what each part is. When you are ready, I will quiz you on the name and function of each component. Partners will alternate identifying the name and function of each part I indicate.

After your quiz, you will be tasked with putting the computer back together – be careful throughout this whole process so you know the computer will be functional at the end!

Activity 1-3: PC Part Quiz

Identifying parts and functions is an opportunity for students to earn points on a concept that is relatively easy to learn and apply. I like conducting the quiz as a hands-on activity; I will pick up each of the 8 most important components and ask students to identify either name or function.

I typically grade students as a pair. The first student identifies the name of the first component and the second student identifies its function. Then the second student identifies the next component and the first identifies its function, such that students are alternating identifying name and function. Students typically study well with one another and both students do well, but if a student does not know an answer, their partner can recover half of a point for the team before I tell them the answer.

Materials

- *See Activity 1-2*

Component Name	Component Function
Power supply	Provides power to other components and converts high-voltage AC to low-voltage DC.
Motherboard	Circuit board which connects to and interacts with all other components
CPU / Processor	“Brain,” conducts calculations
Heat sink	Pulls heat away from the processor to avoid overheating
RAM / Memory	Short-term memory, stores running programs and open documents
Hard drive	Long-term memory, stores documents and files
CD or DVD drive	Read-only removable memory, stores documents and files
Expansion Card: Network Card / Video Card / Sound Card	Adds capabilities not built into the motherboard. The network card allows connection to the Internet or other computer networks. The video card processes images and provides them to a monitor. The sound card turns digital signals into analog sounds speakers can use.

Scoring

I award up to 16 points on this 15-point quiz, 1 point per name/function. I award half-points if one partner can recover an answer.

Activity 1-4: Remanufacturing

The remanufacturing step is wonderfully motivating during the demanufacturing process: when students know that their computer will need to function at the end, they pay attention to detail and take care in handing components.

As students work on re-assembling each part, have them be on the lookout for blown capacitors. Oftentimes when there is an unidentifiable hardware problem, it may tied to a bad motherboard or other component that will need to be replaced due to leaking or bulging capacitors.

Image source: http://img.auctiva.com/

If you have multimeters available, you can also have students test the power output of the button battery included in each computer (~2.9V or higher). If a computer has trouble remembering the date (or you have to reset it with any frequency), the button battery is likely the culprit.

Materials

- *See Activity 1-2*
- Multimeters (optional)

Activity (45 minutes)

When you have completed the quiz, begin putting your system back together. Use care when:

- Touching circuit boards. Remember to equalize electric potential by touching the computer case
- Tightening screws. If you have to force it to fit, it's either not lined up or is not the right screw
- Connecting cables. Some cables look similar but are not the same. Double- and triple-check that the cables fit perfectly before forcing them
- Re-inserting RAM. Each stick of RAM has one or more slots which determine which side goes where. You may need to rotate the stick 180 degrees for it to fit correctly. Ram is properly inserted by pressing straight down on the stick using your thumbs. As long as the side latches are open when you start, you should not have to close them – the RAM will close them for you.
- Plugging case connectors into the motherboard. Many motherboards are connected to the power switch, reset switch, and LED indicators by a number of very small 2-4 pin cables. These connectors are typically located in the corner of the motherboard, and labels typically appear nearby. The location of pin 1 is always labeled on the motherboard and the location of pin 1 on the cables is always indicated with an embossed arrow. This arrow should be pointed at pin 1 on the motherboard.

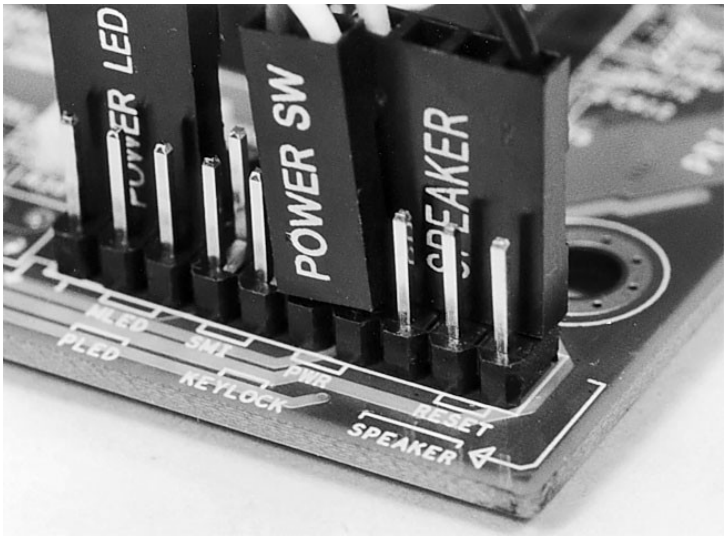


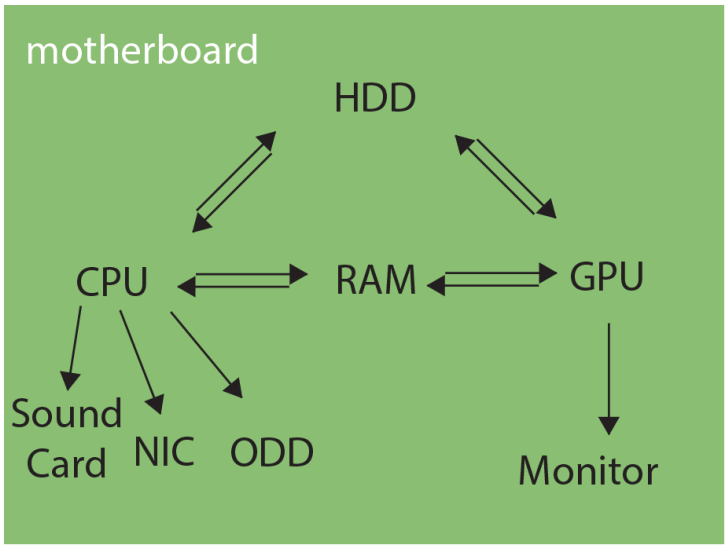
Image source: http://www.pcguide.com/

Activity 1-5: PC Part Mobile

If you want students to truly understand the function and interaction of computer components, they can create a representation of how the components are interconnected.

If you have access to a smattering of spare wire hangers, one way to do this is by having students create a computer component mobile.

This is also a great way to integrate art and higher-level thinking.



One possible interpretation of a computer map

Materials

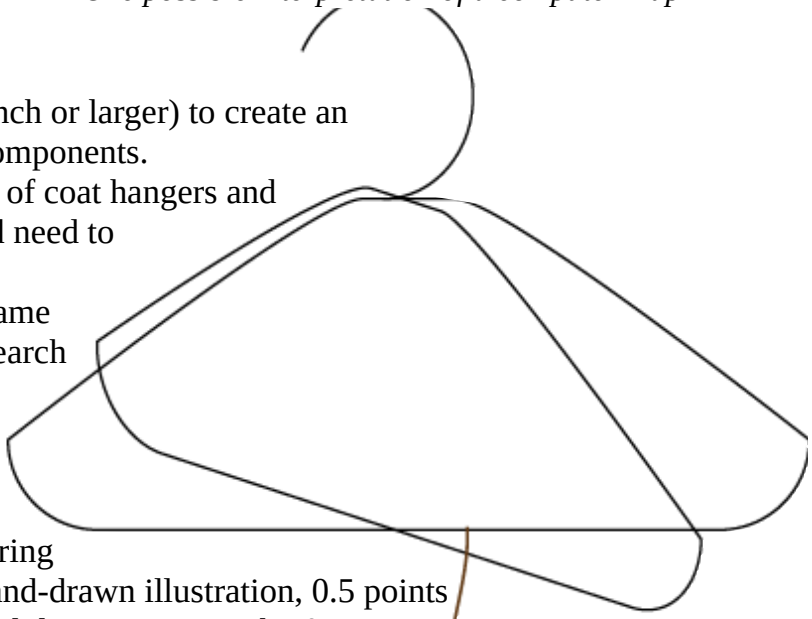
- Notecards
- String and/or Yarn
- Two wire hangers per group

Activity (45m)

In groups of two, use notecards (4x6 inch or larger) to create an illustration and description of 10 computer components.

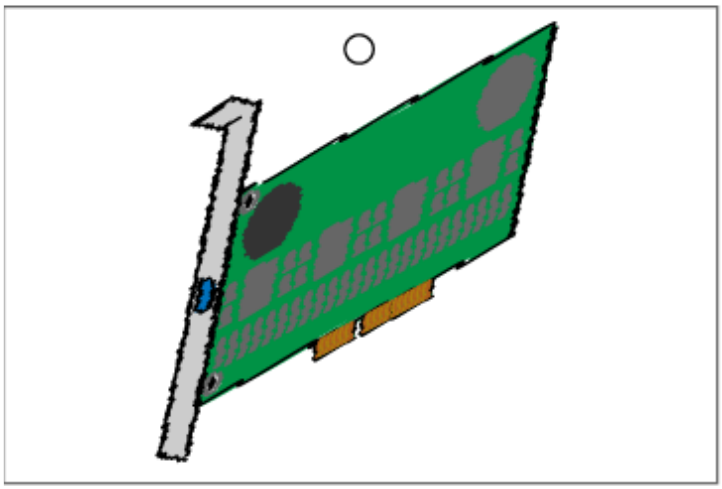
Use string to attach each card to a pair of coat hangers and use yarn to connect components which would need to communicate frequently with each other.

Descriptions can be as simple as the name and function, or you might conduct some research to identify more information, such as types available.



Scoring

Scoring depends on requirements. During one implementation, I awarded 1 point per hand-drawn illustration, 0.5 points per detail / example, and 1 point per functional description. With 10 points for connections, students could earn up to 40 points.



Video Card / Graphics Card (GPU)
Function: to process images and provide them to the computer monitor.

Common connections:
- VGA (15-pin)
- Svideo (9-pins)
- DVI (19-29 pins)
- HDMI (19-29 pins)

Manufacturers:
- nVidia
- ATI (AMD)

Module 2: Hardware to Software

This module helps students understand the progression of instructions required to let a computer's hardware and software function as expected.

Activity 2-1: The Basic Input / Output System

The BIOS is the most basic version of software used on any computer. Since the BIOS can be used to make fundamental changes to a computer system (such as enabling and disabling sound and other functions), it makes sense for any exploration of computer software to start here. You can use the BIOS to learn if the computer "sees" the hard drive, CD/DVD-Rom drives, and other components. The BIOS can be frequently used to help diagnose hardware problems by enabling or disabling components.

Materials

- Part C: Functional computer systems with accessible BIOS (1 per 2 students)

Activity, Part A (5m)

When turning a computer on, you might see a screen filled with text, or you might merely see a logo appear on-screen for a few seconds. What you're seeing is evidence of the BIOS, or the computer's Basic Input Output System. This is the most basic set of instructions your computer has for understanding what is connected to it.

The most important part of the BIOS, and the part that we see flashing before our eyes, is the Power On Self Test (POST), where the computer checks to see that the necessary components are plugged in and functional. *Do I have a processor? I do. Do I have memory? I do, so emit one beep. Do I know that 2+2=4? Excellent.*

What are some other checks the computer might perform?

I have conducted the following activity as part of a brief, whole-class discussion, but it is also something that might work well in small groups to get a larger number of students involved. I use the following analogy for the POST involving my mechanical pencil. I carry mechanical pencils in my pocket, so I occasionally pat my pocket to make sure I haven't left my pencil behind. When I pull a mechanical pencil out of my pocket, I press the plunger to release lead as I watch the end. I always look to see that there is lead before I try writing on a piece of paper. Similarly, I always check that no lead is exposed before putting the pencil back in my pocket.

Activity, Part B (10m)

Whether or not you think about it, you go through many self-tests each day. You might check to see if you have brought a pencil to class, or you might check the time (just to make sure you're in the right place).

Let's see if we can write some questions we might want to perform before we begin class every day. Do you have any ideas? *[Check pencils, fill out planner, check that seat is unoccupied and that desk is clean, complete bell-ringer activity, etc.]*

Activity, Part C (10m)

In addition to watching what the computer does during its POST, we can change many BIOS settings. Take a few minutes to explore the options available (but do not save any changes!). There is often a description or help item for each menu item, but if you cannot find what a function might do, make a list of those items so we can discuss them as a whole class.

Activity 2-2: Operating Systems, History, and Development

Building up from the BIOS, it is important for students to understand the role that the operating system plays, and for students to recognize that there are many different operating systems available.

Materials

- Copies of or student access to *Operating System Timeline* (page 30)
- Functional computer systems with Internet access

Activity, Part A (15m)

The operating system is a much more complex set of instructions that take a hand-off from the BIOS in order to make your computer functional. While the BIOS knows there is a hard drive plugged in, it typically does not have the proper instructions to see what is stored there. Operating systems like Windows and Mac OS on the desktop or Android and iOS on your mobile device allow you to interact with the information stored on your hard drive and to send and receive information on the Internet. Most operating systems include a graphical user interface (GUI), but this is not required: PC-DOS, MS-DOS, and UNIX are all operating systems that have a command-line interface instead of a GUI. These operating systems are still powerful and can still be used today.

The three primary consumer desktop operating systems to date are Windows, Macintosh, and Linux (Linux has many different "flavors" including Ubuntu, Linux Mint, and Fedora / RedHat). The handout, *Operating System Timeline*, in front of you shows the different major releases of these three operating systems. What trends and comparisons do you notice?

- *The first release in each family (MS-DOS and Unix) was text-based (no GUI).*
- *Both Mac OS and Linux are based on Unix, though the earlier versions of Mac OS (1-9) were independent.*
- *Mac OS, like Mac OS X began with an annual release before becoming less frequent. Mac OS X has returned to an annual release schedule.*
- *Windows has had the least consistent release schedule.*
- *Linux was initially released while it was in "beta," in version 0.11. Linux versioning was fairly consistent in later versions: the main number reflected very large architectural changes (1.0, 2.0, 3.0) while point releases are even-numbered (3.0, 3.2, 3.4).*
- *After version 3.4, Linux jumped versions but stuck with the same pattern of even-numbered point releases (3.10, 3.12, 3.14).*

Activity, Part B (25m)

While our observations in Part A are valid, they don't tell us too much about how each operating system has actually changed over time. Was Windows 98 a big step up from Windows 95? Was Windows 98 SE (second edition) a big step forward from Windows 98?

Choose a series of operating systems: Windows, Mac OS, or Linux, and do some research to see what the major features of some versions were. Attempt to answer the following questions using online resources at your disposal:

- Are the features included in each release equivalent?
- Did the goals of the operating system change significantly at any point?
- How has competition between your OS and Windows / Mac OS / Linux impacted development?
- If you have time, how has pricing changed between versions? Is there reason for those changes?

Activity 2-3: Applications

Applications, programs, or apps are pieces of software that are built to run on a specific operating system. (Software packages that run on Linux, Mac, and Windows are usually built for that specific operating system, or are built for a platform like Java. Java in turn must be specifically configured to work with the Linux, Mac, or Windows operating systems.)

Examples of applications range from the very basic Notepad in Windows to the more advanced Adobe Photoshop. These applications cannot run without the framework provided by the operating system.

In addition to traditional applications, there are very specialized applications called drivers. Drivers are the sets of software instructions that give the operating system detailed information on how to use a specific piece hardware.

Materials

- Functional computer systems with a fair amount of RAM (More than 1GB)
- Ubuntu Linux Live CD/DVDs, 1 per station
- Copies of the *Software Evaluation Rubric* (page 31, optional)

Activity (40m)

Operating systems do not always have to be installed on a computer in order to run, though they usually are (and work best this way). Today we are going to use an operating system equivalent to Windows without installing it on our computers; we are going to run what we call a Linux Live CD. No files are installed on the computer. Instead, the operating system is stored in the memory (RAM). As you may recall, once we turn the computer off, everything stored in the RAM will be gone, as will our temporary operating system.

Insert your CD into the drive and turn off your computer if it is not already off. Turn it on again.

Caution: Depending on your computers' configuration, Linux may immediately load from CD/DVD or you may need to push a key to see all boot options, and select the CD/DVD drive from there. In very rare circumstances, you may need to go into the BIOS to move the CD/DVD up in the boot sequence.)

Since the whole operating system is being loaded into memory, this may take a moment.

Debates over the most popular Linux “flavor” distribution rage on, since there is no good way to monitor usage, but nearly any list you find will include Ubuntu Linux in the top 3. Ubuntu is generally thought to be a good distribution for users who are new to Linux, and since it is easy to set up we will be using it today.

Ubuntu, like the mobile operating systems Android (Linux-based) and iOS (Unix-based), has an “app store” called the Ubuntu Software Center. As we seek to examine the applications that we run on computers, I will let you explore the different types of software available on Linux. Many of the programs on Linux are available for Windows and MacOS as well: some you might recognize as you browse the software center.

As you browse, you are welcome to try installing a few applications, but note that our operating system is running on our computer's RAM, which does not allow a lot of extra space for large applications, and that none of the applications will be running at full speed. It would be worth your time to look at the program's size before attempting to download and install it.

Caution: Depending on your network configuration, you may need to have students visit System Settings > Network > Advanced in order to enter proxy settings. This is definitely an activity to try ahead of time!

Activity 2-4: Writing Instructions

There is no single activity that parallels writing a detailed computer program, particularly that can be completed in a single class session. To get students thinking about the level of detail that might be required to write a computer program, however, I invite students to teach me how to make a nice, messy s'more. They quickly discover that their instructions must be VERY detailed, otherwise I will find a loophole and complete the task in a way different than they intend.

Materials

- Butter knife
- Chocolate chips
- Graham crackers
- Marshmallow fluff

Activity, Part A (15m)

I had a few items left over after my Halloween party a few weeks ago, so I thought you might like to help me make some s'mores. There is a small catch, however: I've never made s'mores before, so you'll have to tell me what to do. [Have different students give instructions from their seat, and pay attention only to verbal instructions. Make as many mistaken interpretations as possible – it can be frustrating to the student who is giving instructions, but it's entertaining for everyone else!]

After approximately 15 minutes, or sooner if students have largely become successful in giving instructions, I ask students to explain why I did this activity.

Activity, Part B (10m)

Why did I have so much trouble following simple instructions? *The instructions were not clear enough, or more likely, I didn't understand the operational definitions of the words you used.* Computers sometimes have the same problem: computers can only do exactly what they have been programmed to do. Most programming languages have clearly-defined functions that would have avoided some of today's problems, but as you have probably encountered in your own life, there are mistakes that are made by the humans who write the programs we use every day. How do you think software developers might try to minimize their mistakes? *They often inspect each others' work, software usually goes through both automated (machine-driven) and manual (human) testing.* Unfortunately, not every mistake can be caught, which leads to “bugs” or “vulnerabilities” found in software.

Activity 2-5: Bug Hunting

Bugs are a natural part of any human-made computer program, but it is hard to appreciate the extent to which bugs affect software and the process which developers must go to in order to address them. Having students spend a few minutes exploring the bug tracker of LibreOffice, Pidgin, or another open source project gives students a bit of perspective to see what processes bug hunters and developers go through to produce a good product.

Materials

- Functional computer systems with Internet access

Activity (15m)

Bugs are an unfortunate reality in any piece of software. Computer programs are written by humans, and they bring with them human error. The number of bugs varies. Microsoft Windows XP Profesional, for example, according to Secunia's March 2015 statistics, has had 446 security advisories and 668 vulnerabilities since 2003. Windows is a large piece of software (and this count does not include the number of vulnerabilities in Internet Explorer, which is built-in), so each vulnerability could affect hundreds of lines of code. Smaller pieces of software (for example, Microsoft Paint) will see many fewer bugs.

So how do bugs get identified and corrected? Many bugs are reported by the users of the software, just as many features are requested by users. Every software developer has some way to receive and address problems in their program. Some developers automatically test software using a variety of security tools, but most programmers rely extensively on user testing.

Today you are going to take a few minutes to see what bug reports might look like in the real world. Many open source or community-developed software applications make their bug reports public, and one example is LibreOffice. You will visit a web page which lists the current, unfixed bugs in the software.

https://bugs.freedesktop.org/buglist.cgi?field0-0-0=blocked&resolution=---&type0-0-0=anywordssubstr&value0-0-0=75025

You can see how bugs are organized, so that someone can focus on addressing all the bugs in one component or concentrate on the most critical items. Items which are being actively fixed are assigned to a specific person. The summary links take you to a page with more information, including conversations back and forth between different developers describing how the problem was identified and what might be done to fix it.

Activity 2-6: Installing and Accessorizing an OS

Like the computer components hidden inside a computer case, it is hard to understand how the operating system interacts with the BIOS, with drivers, and with applications until you have had an opportunity to go through it yourself.

Installing Windows, addressing problems with missing and out-of-date drivers, and seeing how many windows updates have been released can help students not only recognize the complexity of the systems we use every day, but can also help them troubleshoot problems they encounter with their own system.

Materials

- Remanufactured computers from Activity 1-4 and related hardware (keyboards, monitors, and mice).
- A workspace in which to plug in the computer tower and its peripherals.
- Windows XP or Windows 7 CD / DVD
  Windows XP will almost certainly require downloading drivers in order to get the system fully-functional, especially sound and network drivers. This can be very frustrating but could be illuminating to some students. Windows 7 is much less likely to require critical drivers, but will certainly require driver updates.
- Student copies of *Internet Security*, pages 34-44. Students will have considerable downtime while working in which they can begin work on Module 3.

Activity, Part A (10m)

The time has come to test and see if the computer you re-manufactured is in working order. In order to begin today, you will want to check and make sure that your computer tower is completely reassembled:

- Are all cables connected on both ends (with the possible exception of some cables coming from the power supply)?
- Do information devices (CD/DVD drives, hard drives, and floppy drives) have both a power and data cable connected on both ends?
- Are the motherboard / case connectors correctly installed? Does the motherboard have two power connections?
- Do all of the fans have power? You need to keep your computer cool!

When you think your computer is completely ready, please get my attention so I can check over it with you. If I think you're ready, I will give you media (CD/DVD) to install Windows as well as an *Internet Safety* reading.

It is important to double-check students work at this stage. While unlikely, it is best to avoid cables plugged into an incorrect slot and avoid any risk of “frying” a computer or component.

If students completed Activity 2-3 and are still working in partners, they should be able to boot the computer to the Windows disc.

Activity, Part B (40m)

As you are installing Windows, answer any questions you need to (usually with the default answer) in order to complete the installation. As long as your media is Windows XP Service Pack 3 or later, you will not need to enter a product key during installation – you can use (most features) of Windows for 30 days without activation. As your computer is installing the necessary software, please begin reading the *Internet Safety* packet I have provided.

Module 3: Internet Safety

The Internet safety module orients students with digital threats and equips them with the knowledge and tools to proactively protect computer systems.

Activity 3-1: Your Computer as a Target

Everyone has heard that hackers want access to their computer, but why would they? A good discussion about malicious motives makes the entirety of Module 3 relevant to students. Students gain an understanding of motives when money is brought into the fold. To take this topic deeper, you can generate a great discussion by conducting a short social engineering reading. Kevin Mitnick's *The Art of Deception* is a fascinating read, but the two-page excerpt I refer to below will be all the impetus students need to delve more deeply.

Materials

- A teacher copy of *A Classic Case of Deception* from Kevin Mitnick's *The Art of Deception*, published by John Wiley & Sons, 2002, included on page 33.

Activity, Part A (15-30m)

Why do you think anyone would be interested in gaining access to your computer? The average person does little more with their computer than write e-mails and check Facebook.

- *Some people do online banking, and many people do online shopping. Access to banking or credit card information is worth money!*
- *Even if a hacker wouldn't be interested in your Facebook page, the password that many people use for Facebook is the same as their bank password or their Amazon account...*
- *Access to your Facebook account allows a malicious user to use your account to spread spam, or unwanted advertising messages. Spammers pay good money for good accounts to spam from, because someone always seems to be convinced that they can get a free iPad if the idea appears to come from the right person (you)!*
- *Your whole computer could be hijacked to perform spamming functions (to make the hacker money), or to perform other functions like launch dedicated denial of service (DDoS) attacks (again for money or political reasons).*
- *Information on your computer (or your Facebook account) might be salable. If you've been making a list of your friends' social security numbers, for example...*
- *Gaining access to your computer could expose your whole network, and while your computer might not contain valuable information, your boss's or parents' could!*

There are many reasons that malicious hackers might be in their trade. They may enjoy the thrill, they may enjoy proving how smart they are, but most often they are looking for what? *Money!* Of course, hacking can sometimes be done without a computer, which is what we now call social engineering.

(Optionally, you can read and generate a discussion based on the included social engineering reading.)

Activity, Part B (5m)

Despite concerns for our information, many people don't think twice about transmitting important information wirelessly. Unfortunately, even wireless access points with WEP and WPA encryption (which require passwords for use) may not be enough for a committed hacker in a van outside your home.

There are many steps you can take to secure your wireless transmissions:

- Use WPA2 encryption with strong passwords. Strong passwords might be entirely random letters, numbers, and symbols, ideally 25 characters long (or longer!). WPA2-PSK supports passwords of up to 63 characters.
- Change the default administration password and disable remote router administration by turning the “allow admin via wireless” option off.
- Change the default network name and disable SSID broadcasting. This requires any users to know the access point's name rather than simply choosing it from a list.

Of course, the best recommendation related to wireless security is to be careful about what is done wirelessly. If you are banking or shopping online, or if you are logging onto an e-mail account which is tied to banking information, these tasks are best accomplished on a wired connection.

Activity 3-2: Internet Safety Reading

Internet safety can be a very inclusive term, but it all ties back to maintaining a secure computer. The included reading is a revised copy of the Computer Banc Internet Safety Manual, which was used as part of an Internet safety course. It was created in the era of Windows XP (and still includes images of a Windows XP system), but text has been updated to remain relevant in Windows 7 and beyond.

Materials

- Student copies of Internet Security, pages 34-44.

Activity (30-40m)

This activity is ideally completed as part of Activity 2-6.

Activity 3-3: Internet Safety Applications

This content directly follows Activity 2-6. After installing Windows, having students install an anti-virus and other programs is a very useful exercise, as it familiarizes them with the process and several interfaces.

Materials

- Remanufactured computers from Activity 2-6 and related hardware (keyboards, monitors, and mice).
- A workspace in which to plug in the computer tower and its peripherals.
- Group copies of *Installation and Configuration To-Do List*, page 32.

Activity

With Windows installation complete, follow the steps outlined on the *Installation and Configuration To-Do List* I have provided. You may not be able to accomplish all tasks in the time provided, but do try to complete as many as you can. (The first things to skip if you're feeling rushed for time is running scans.) Since this is a fresh installation of Windows, we can hope that our systems are still clean. Of course, this is only a hope – because we did not install Windows updates, there are many unpatched vulnerabilities in Windows.

Caution: download sites (and downloads themselves) are commonly blocked at schools. You may want to check with your IT department to see if they are blocked and if they can be temporarily unblocked for this activity.

Students are always rushed with this activity, and I can't usually afford to give them more than 40-60 minutes of class time. The more valuable experiences are provided by Spybot (if students can recognize the value of immunizing), COMODO (because it, like many other good software pages, is bloated with unnecessary tag-along software), and Secunia PSI (this is a great piece of software for students to try out at home).

Activity 3-4: How Your Anti-virus & Firewalls Work

To many, anti-virus and firewall software are driven by pure magic: they can always be trusted to get the job done. In reality, the software we trust to protect us are as fallible as any other software we might use, and in order to avoid the pitfalls we need to understand how these important pieces of software work.

Materials

- Functional Windows computer systems with Internet access and configurable anti-virus / firewall software

Activity, Part A (10m)

Anti-virus programs typically work in three ways.

The most traditional approach is for the virus scanner to search for files (or parts of files) that match a known virus. When an exact match is found, the file is quarantined (moved to a separate memory space where it is not allowed to interact with other files), cleaned (the offending portion of the file is quarantined / deleted), or deleted altogether.

Much like biological viruses, computer viruses change rapidly, adapting so they cannot be detected by anti-virus signatures. Heuristic scanning allows anti-virus programs to investigate the similarity of files to known viruses. Depending on similarity and sensitivity settings, the anti-virus program may then quarantine, clean, delete, or ignore each file. Many anti-virus programs are designed to send suspect files to the anti-virus provider (eg. McAfee or Symantec) for further testing and possible inclusion in the next set of virus signatures.

Behavior-based anti-virus scanners watch what each software application on the computer does, and compares each and every application to a whitelist of known safe programs. Depending on your settings, the anti-virus may ask you if you want the program to run, or it may alert you when the unknown application tries to install a "hook" to capture keyboard events (as a keylogger would do) or when the unknown application accesses many files on the computer (as spyware might do).

Based on what you know about viruses, spyware, and malware, what other types of behaviors might be suspicious?

Activity, Part B (20m)

In order to understand how firewalls work, we need to better understand network traffic. In this activity, we are going to perform a variety of very basic network diagnostics in order to gain an understanding of how firewalls make decisions to allow or deny traffic.

First, log into your computer and load command prompt. You might be able to type `cmd` in the start menu search bar, you might be able to type `cmd` into Start > Run, or you may need to navigate to Start > All Programs > Accessories > Command Prompt.

Caution: access to tools like the command prompt is sometimes blocked to student users. You may want to check with your IT department to see if command prompt is available to students or can be temporarily made available for this activity.

In the command prompt, type `ping google.com`. If you receive a response as on right, you have successfully connected to the server you intended to. As you can see, each server on the Internet has a specific IP address, and

```
Pinging google.com [74.125.225.128] with 32 bytes of data:
Reply from 74.125.225.128: bytes=32 time=19ms TTL=53
Reply from 74.125.225.128: bytes=32 time=19ms TTL=53
Reply from 74.125.225.128: bytes=32 time=19ms TTL=53
Reply from 74.125.225.128: bytes=32 time=20ms TTL=53
```

firewalls use the IP address (along with other pieces of information) to determine if network traffic is legitimate or malicious.

Caution: School content filters sometimes block web sites by domain name only. This activity could expose a work-around to your students, as typing in 74.125.225.128 in the address bar would let them access Google or typing 173.252.120.6 could let them access Facebook.

Also in command prompt, type `tracert google.com`. This will let us trace the route our information takes from this computer to Google's server and back. As you can see in the example below, our information typically travels through 10+ servers on its way between us and our destination.

```
Tracing route to google.com [74.125.225.131]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  192.168.2.254
  2     6 ms     7 ms     5 ms  66-      -1.adsl.pe  il.grics.net [66.      .1]
  3    40 ms    53 ms    18 ms  peknil-sth-lumx20-03.grics.net [64.40.75.33]
  4    13 ms    15 ms    12 ms  206.51.89.219
  5    45 ms    13 ms    13 ms  bb-mrghmoqa-jx9-02-ae0.core.centurytel.net [206.
51.69.2]
  6    19 ms    19 ms    18 ms  bb-chcgilwu-jx9-02-ae8-0.core.centurylink.net [2
04.9.121.190]
  7     *        *        *     Request timed out.
  8     *       19 ms    19 ms  cer-edge-18.inet.qwest.net [67.14.122.10]
  9    20 ms    20 ms     *     208.47.121.146
 10    23 ms    29 ms    20 ms  209.85.255.132
 11    21 ms    26 ms    21 ms  209.85.240.152
 12    21 ms    20 ms    20 ms  ord08s09-in-f3.1e100.net [74.125.225.131]

Trace complete.
```

Firewalls can look at the path a packet takes to see if there is anything suspicious.

Firewalls also look at the type of data enclosed in each packet, and look to see if we requested that data or if it showed up unannounced.

Firewalls are typically designed to compare data packets to a set of rules, and can accept or deny packets depending on specific rules or levels of suspicion. A firewall can be used to block non-secured web traffic received on port 80, for example, or mail traffic on port 25 if the computer is not a mail server. It can reject traffic from known bad servers by IP address or based on malicious content in the packet. A firewall can use suspicious characteristics (like unexpected data or mislabeled data, such as FTP traffic disguised as HTTP traffic) to decide whether or not to reject packets as well.

Both anti-virus and firewall programs have a multitude of settings that can be used to configure their sensitivity and behavior. Take a few minutes to explore the settings of the anti-virus and firewall programs installed on your computers. What could you do to loosen or tighten security?

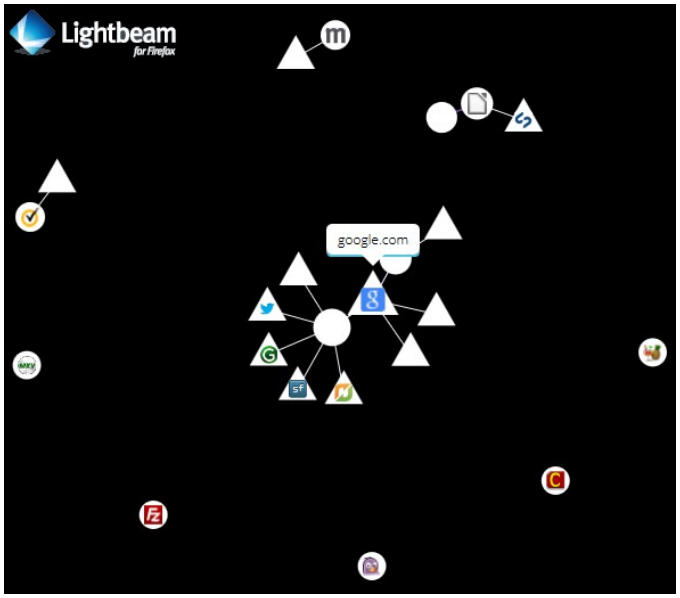
Activity 3-5: Tracing Your Own Tracks

As we use computers, they track our activities. Oftentimes this logging is done to enhance our experience, but other times tracking is to our detriment. This activity is intended to give you a glimpse of what information your web browser is keeping and how that information is being shared.

Materials

- Computer systems with Lightbeam (Firefox), Collusion (Chrome), or a similar browser extension installed.

Activity (20m)



As you may recall, cookies are small pieces of information stored by your web browser on behalf of the web sites you visit. Cookies can be useful (they remember that you are logged in, for example), but they can also be used somewhat maliciously. Cookies can be used to track your every movement, and they can sometimes be used by adware and malware to learn about your interests and habits or to provide relevant ads.

So how bad can this get? Many web sites share information with each other or third-parties (parties whose site you have not visited). In order to trace your own tracks, open Firefox and find the Lightbeam icon on the toolbar. Click this icon to bring up a graph of activity so far. If there is any, clear it using the Reset Data button on the left side of the screen. Then visit a variety of web sites, especially e-commerce sites. You might look to buy a new computer, a new pair of shoes, and a case of your favorite candy bars.

Caution: shopping sites are commonly blocked at schools. You may want to check with your IT department to see if they are blocked and if they can be temporarily unblocked for this activity.

Click back on the Lightbeam icon and see how your graph looks. What sites have shared information with each other? Think about it... what do your experiences at one retailer tell another retailer about you?

To protect your information, it is often good practice to set your browser (Chrome, Firefox, Internet Explorer, Opera) to do several things, each of which builds on the item before it:

1. Send a Do Not Track request to each site you visit.
2. Refuse third-party cookies.
3. Regularly use anti-spyware programs like Spybot: Search & Destroy to remove tracking cookies.
4. Clear all cookies every time you close the browser.

Activity 3-6: Menu of Recommendations

Based on everything you have learned so far, what are the most important steps a person can take to protect their computer and its information?

Materials

- Paper and pencil or a computer with a word processing program

Activity (30m)

We have learned about a lot of items so far, particularly in relation to how we can keep our computer and information safe. In small groups, I would like you to take some time and decide which steps are the most important. Choose 10 recommendations that you think every person should do or have done for their computer – these can be passive tasks like installing a firewall or active tasks like performing an anti-virus scan weekly. Explain why this task is important and be specific in your recommendations so that someone could use your list to perform that task.

For example:
Update Spybot Immunizations weekly. There are many sources of malware on the Internet, but blocking your computer from accessing those sites might stop an infection before it can occur. Every 7 days (or more often), open Spybot: Search and Destroy and click the Immunization button. Click Apply Immunization.

Scoring

I have scored this assignment so students can earn up to 30 points: 1 point per item for identifying the recommendation, describing their concern, and describing the process of resolving that concern.

Module 4: Troubleshooting

While the first three modules focus on background knowledge and preventative steps, this module provides students with the final tools they need to fix existing problems.

Activity 4-1: Troubleshooting a Network

The most common source of trouble at the residential level is an Internet connectivity problem.

Materials

- Student copies of *Network Troubleshooting Guide*, page 45.
- Blank Paper for creating flowcharts.
- Computer systems with various network problems (optional).

Activity (20-40m)

Today we are going to look through a *Network Troubleshooting Guide* to see if we can solve a connectivity problem. While the guide is helpful, it may be even more valuable to create a flow chart to clarify the different steps we can perform. Working in partners or in small groups, you will have approximately 10 minutes to put together a flowchart for wired and wireless connectivity problems. See if you can include a few decisions to make as you troubleshoot: for example, is it just Internet connectivity that is a problem, or is connectivity in general a problem?

After students have completed flowcharts, have them share their ideas with each other. If you are able to mimic network connectivity issues (disable a network device, unplug a cable) and time permits, it is always instructive to see how well the students can actively troubleshoot.

Activity 4-2: Aim to Infect

The second most common source of trouble at the residential level is infection with a virus / spyware / malware. The European Expert Group for IT Security has worked with various anti-virus vendors to add definitions for a test file – a completely safe but detectable virus. Allowing students to use a virus scanner to detect this file gives them real-world virus experience without introducing an actual threat to your network. For more detail on the virus test file, visit http://www.eicar.org/86-0-Intended-use.html.

Materials

- Functional computer systems with running anti-virus and the EICAR test file, accessible at http://www.eicar.org/85-0-Download.html

Activity (15m)

Your computer has been behaving strangely over the past few days. What are you going to do?

Activity 4-3: Trading Clutter for Speed

As times goes on and computers are used, they tend to get cluttered. This is true of all operating systems, but is especially true of Windows operating systems.

Like many computer topics, this phenomenon is best illustrated by having students conduct scans and identify the number of items that can be "cleaned."

Materials

- Functional Windows computers with COMODO System Utilities and administrator access (https://www.comodo.com/home/support-maintenance/system-utilities.php)

Activity (20m)

There are many places that information is stored on a computer. In Microsoft Windows, the operating system as well as many different programs will save settings, image previews, and other "bits" of information in one of several places: as part of the registry (a database of different small pieces of information, many of which determine how Windows itself runs), as part of a configuration file, or as a raw file on the hard drive.

To get a glimpse into what programs are running on the computer, go to the control panel (Start > Control Panel) and select Programs and Features or Add/Remove Programs. Take note of how many programs are installed.

To get a glimpse of what is running when the computer starts, go to MSCONFIG (Start > Run > msconfig.exe) and look at the Startup tab. Optionally you can also look at what services run when the computer starts (Start > Run > services.msc). Each service has a startup type: "Automatic" means it runs when the computer starts, "Automatic (Delayed)" means it runs when the computer has started and is not too busy, and "Manual" means the service will only run when needed. (Changing service settings is not recommended unless you are truly experienced, but it is interesting to see how many services run on startup.)

To begin cleaning the computer safely, run Windows Disk Cleanup (Start > Run > cleanmgr.exe). Select the primary hard drive (usually C:\) and run a scan. By default this tool only cleans a few areas, and removing any of the listed items should be safe. (That being said, there is some benefit to keeping Windows Error Reporting information as well as Setup Log Files.) There is also a button labeled "Clean up system files," which re-runs the scan in more locations, including Windows Update, Device Drivers, and further memory dumps. Deleting these items is not usually recommended.

Any further cleaning can be risky, but there are many tools specifically designed to clean unnecessary registry entries or other files (CCleaner is probably the best-known tool). Most tools make a backup before deleting items, but each tool is known to have made mistakes. Today we will run a scan but not perform any actual cleaning to be safe. Conduct a scan using COMODO System Utilities. The scan will find registry entries which might be deleted, privacy items (including cookies and file access logs) which can be deleted, and files (such as thumbnails and some configuration files). Look through the results of each cleaner and see what it is recommending you do (but don't do it!). Note that many items are left unchecked because deleting those items is not usually recommended. As with any cleaning experience, it is very important that you understand what the program is doing before you click on "Clean."

Activity 4-4: Troubleshooting Printers

There are a wide variety of problems that a user can face when having printer problems. This activity describes a few general problems faced when printing, but many printing problems may be specific to the manufacturer. The guide largely applies to consumer printers rather than copiers and multi-function devices.

Materials

- Student copies of *Printer Troubleshooting Guide*, page 47.
- Printers with various network problems (optional).

Activity (15m)

When a document is printed, it gets translated several times before it is printed, and problems can occur at any step along the way. There could be a problem with the program (eg. Microsoft Word), with the driver, with the operating system (eg. Microsoft Windows), with the network or connection between the computer and the printer, with the printer's operating system, or with the printer itself. As such, troubleshooting a printing problem can be complex, though many problems can be fixed by restarting the computer and/or printer. You can use the provided Printer Troubleshooting Guide to solve many common problems.

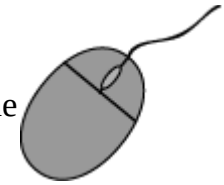
Computers and Their Components

The **hardware** of a computer is any part of the computer that can be physically touched, from the computer case to the monitor and other peripherals. **Peripherals**, or optional devices which work cooperatively with the computer system, include the keyboard, mouse, and printer.

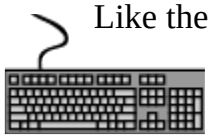
Software is a set of instructions which cannot be physically touched – they exist only in memory. While you might think the parts you can touch are more important, hardware and software are equally important. Without software, hardware would not know what to do; without hardware, software would have nothing to process its instructions.

External Hardware

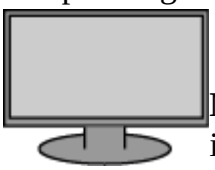
The parts of a computer that we are most familiar with are those that exist outside of the computer case – the parts we see, touch and interact with. Among the most important items are the mouse, keyboard, monitor and printer.



The computer mouse is one of a computer's **input** devices, which allows a user to provide information to the computer system. The **mouse** allows a user to control the cursor (pointer) on the computer screen as well as click or scroll. Alternatives to the mouse include a touchpad (which you will typically see on a laptop computer), a trackball, and the touchscreen.

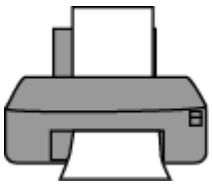


Like the mouse, the **keyboard** is an input device: it accepts user input but does not provide any direct feedback to the user. In addition to numbers, letters, and symbols, the keyboard includes function keys and can control the computer system through the use of keyboard shortcuts. Pressing F5 in a web browser will refresh the page, for example, and pressing Ctrl and S at the same time will typically save a document.



Other input devices include scanners, cameras, and tablet devices.

The monitor is an **output** device, because it provides information to the user. **Monitors** can be of many different sizes and styles, but they all provide visual information to the user. (A monitor can also be an input device if it is a touchscreen monitor.)



Similarly, **printers** provide information output on paper. A speaker is also an output device, though it provides audio information instead of visual information.

Internal Hardware

Inside of the computer case are many different **components**. Some are completely hidden by the computer case while other parts, such as CD/DVD drives, are partially visible.

One of the most important components is the power supply. The **power supply** unit (PSU) takes energy from wall outlets and converts it into a form that powers your computer. (The PSU takes high-voltage alternating current (AC) and converts it to low-voltage direct current (DC).) The PSU has a single cable connecting it to the wall and many cables inside the computer case so each component can have its own source of power. (Many components, including the motherboard, actually need multiple connections to the power supply.)

The **motherboard** holds everything else together. It has slots for the processor, memory, and expansion cards, and also has connections for hard drives, disc drives, and other peripheral ports like USB. The motherboard is the largest circuit board in the computer. It supports all the other computer components by allowing them to communicate with one another and sometimes even by providing power.

The “brain” of the computer is the **processor**, or central processing unit (CPU). This is the part of the computer that performs calculations large and small, interpreting instructions provided by other computer components or instructions provided by software. The CPU works very quickly, and as a result it can produce a lot of heat. This is why processors are typically covered by copper or aluminum **heat sinks**, which help spread heat quickly, avoiding overheating.

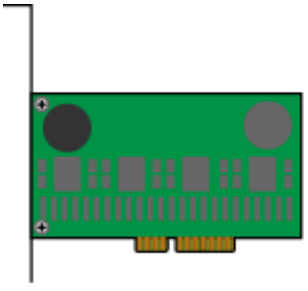
The processor knows how to think, but it does not know how to remember. Therefore, the CPU must work very closely with the computer's **RAM**, sometimes simply called its **memory**. RAM stands for Random Access Memory, which means they can remember any type of information in any arrangement. The software you run (Microsoft Windows or Microsoft Word, for example) is stored in memory while it is in use, as is any document you might type. RAM is the computer's short-term memory: it tends to be limited, and as soon as your computer loses power the information stored in RAM is lost. Thankfully, you can save information to long-term storage which is not lost when you turn the computer off or if power is lost.

The **hard drive** or hard disk drive (HDD) stores information for a long period of time. This is where you save documents or other files like music or movies, and where software is stored. A newer form of hard drive is the solid state drive (SSD), which uses flash memory rather than traditional magnetic memory. Solid state drives tend to access and move data much more quickly than traditional hard drives.

The hard drive typically stays in place inside the computer case, but there are also a variety of forms of **removable memory**, which are meant to be added and removed as you play a game or watch a movie. One example of removable memory is an optical disc drive (ODD) such as a CD-ROM or **DVD-ROM**. Unlike RAM, which can both read and write information, these types of read-only memory (ROM) cannot typically be changed. Information, once stored, is stored forever unless the media is specifically designed to be re-writable (as in the case of CD-RW and DVD-RWs). **Flash drives**, which commonly use a USB connection, are easily removed, but like RAM or internal hard drives they can be both read and written to a large number of times.

Each of the internal hardware components we have described so far plug into the motherboard either directly (in the case of the CPU and RAM), or indirectly via a cable. Motherboards also feature slots for expansion cards, such as a modem, network card, and sometimes a sound or video card.

A **modem** connected directly to the motherboard is used where broadband Internet access is not available – a telephone line plugs into the card, which is connected to the motherboard. A **network card** (or network interface card, NIC) is more often used for a wired Internet connection. When a network card is used, a network cable connects your computer to an external cable, DSL, or other high-speed modem.



Sound cards do what you would expect: they process digital sound and provide an analog signal to speakers through ports on the card. **Video cards** process video and provide it to a monitor or other device through their own ports. A **port** is any place where you plug in or connect hardware. Ports outside of the computer case include sound and video ports, network ports, and generic ports like USB or Firewire.

Operating Systems Timeline

1969		Unix	Unix
...			
1981	MS-DOS		
1982			
1983			
1984		Mac OS 1	
1985	Windows 1.0	Mac OS 2	
1986		Mac OS 3	
1987	Windows 2.0	Mac OS 4 Mac OS 5	
1988		Mac OS 6	
1989			
1990	Windows 3.0		
1991		Mac OS 7	Linux 0.11 (Unix-like)
1992	Windows 3.1		
1993			
1994			Linux 1.0
1995	Windows 95		
1996			Linux 2.0
1997		Mac OS 8	
1998	Windows 98		
1999	Windows 98 SE	Mac OS 9	Linux 2.2
2000	Windows 2000 Windows ME		
2001	Windows XP	Mac OS X.0 (Now Unix-based) Mac OS X.1	Linux 2.4
2002		Mac OS X.2	
2003		Mac OS X.3	Linux 2.6
2004			
2005		Mac OS X.4	
2006	Windows Vista		
2007		Mac OS X.5	
2008			
2009	Windows 7	Mac OS X.6	
2010			
2011		Mac OS X.7	Linux 3.0
2012	Windows 8	Mac OS X.8	Linux 3.2 Linux 3.4
2013	Windows 8.1	Mac OS X.9	Linux 3.10 Linux 3.12
2014		Mac OS X.10	Linux 3.14

Software Evaluation Rubric

Application Title: _____

Version: _____ Producer / Publisher: _____

Category or Categories (circle): Board Games / Card Games / Puzzles / Role Playing / Sports / Other

Price: FREE Most Appealing Feature: _____

	1 = Poor		3 = Neutral		5 = Great
Game Components					
Graphics	1	2	3	4	5
Gameplay	1	2	3	4	5
Load Time (compared to awesomeness)	1	2	3	4	5
Overall Rating (choose before completing items below)	1	2	3	4	5
Ease of Use					
Directions are Clear	1	2	3	4	5
Game resumes where it stops	1	2	3	4	5
Error Free	1	2	3	4	5
Ability Level					
The software covers a wide variety of ability / skill levels	1	2	3	4	5
Assessment					
The software records user progress	1	2	3	4	5
Feedback is given when the user does something wrong	1	2	3	4	5

Likes: _____

_____

_____

Dislikes: _____

_____

_____

Educational Value: _____

_____

_____

Installation and Configuration To-Do List

Install Windows

Install Drivers

- Right-click on Start > My Computer. Click on the Hardware tab and open the Device Manager. Missing drivers are denoted by a yellow exclamation point.
- Visit the web site of your computer manufacturer (dell.com, gateway.com, hp.com, etc.) and find the "Technical Support" or "Support and Drivers" page.
- Search for your computer's model number.
- Back on the web page, download the newest version of each type of driver for your model and operating system version.
- Install drivers until there are no more yellow exclamation marks.

Update Windows

- Use the link at Start > All Programs > Windows Update
- Check for updates and look at the number of updates that are available. Updates are given different ratings, and you can explore to see what numbers of different update types are available. Pay particular attention to the important and recommended updates. The titles of each update gives you a vague idea what the update does, but the KB numbers are tied with Microsoft's Knowledge Base, which offers more detail.
- Do not actually perform any updates – just look. Note that this may be the first batch of updates, after updating there may be updates to fix updates we just installed.

Spybot: Search & Destroy Free

- Download from safer-networking.org
- Install
- Update
- Immunize

Malwarebytes Anti-Malware (MBAM)

- Download from malwarebytes.org
- Install
- Update
- Quick Scan

COMODO Internet Security FREE (Anti-virus and Firewall)

- Download from comodo.com
- Install carefully. This software, like many others, offers to install far more than you need – feel free to decline GeekBuddy (a remote assistance service) and COMODO Dragon, a web-browser based on Google Chrome. Choose ONLY the Antivirus and Firewall options.
- Update
- Quick Scan

Secunia Personal Software Inspector (PSI)

- Download from secunia.com
- See what programs and drivers might be out of date

MSCONFIG

- Follow the guide to see what programs are loading on startup
- Compare the list of programs to Appendix 1. Which items might be suspicious?

A Classic Case of Deception

An excerpt from Kevin Mitnick's *The Art of Deception*, published by John Wiley & Sons, 2002.

One day in 1978, Rifkin moseyed over to Security Pacific's authorized-personnel only wire-transfer room, where the staff sent and received transfers totaling several billion dollars every day.

He was working for a company under contract to develop a backup system for the wire room's data in case their main computer ever went down. That role gave him access to the transfer procedures, including how bank officials arranged for a transfer to be sent. He had learned that bank officers who were authorized to order wire transfers would be given a closely guarded daily code each morning to use when calling the wire room.

In the wire room the clerks saved themselves the trouble of trying to memorize each day's code: They wrote down the code on a slip of paper and posted it where they could see it easily. This particular November day Rifkin had a specific reason for his visit. He wanted to get a glance at that paper.

Arriving in the wire room, he took some notes on operating procedures, supposedly to make sure the backup system would mesh properly with the regular systems. Meanwhile, he surreptitiously read the security code from the posted slip of paper, and memorized it. A few minutes later he walked out. As he said afterward, he felt as if he had just won the lottery.

Leaving the room at about 3 o'clock in the afternoon, he headed straight for the pay phone in the building's marble lobby, where he deposited a coin and dialed into the wire-transfer room. He then changed hats, transforming himself from Stanley Rifkin, bank consultant, into Mike Hansen, a member of the bank's International Department.

According to one source, the conversation went something like this:

"Hi, this is Mike Hansen in International," he said to the young woman who answered the phone.

She asked for the office number. That was standard procedure, and he was prepared: “286” he said.

The girl then asked, "Okay, what's the code?"

Rifkin has said that his adrenaline-powered heartbeat "picked up its pace" at this point. He responded smoothly, "4789." Then he went on to give instructions for wiring "Ten million, two-hundred thousand dollars exactly" to the Irving Trust Company in New York, for credit of the Wozchod Handels Bank of Zurich, Switzerland, where he had already established an account.

The girl then said, "Okay, I got that. And now I need the interoffice settlement number."

Rifkin broke out in a sweat; this was a question he hadn't anticipated, something that had slipped through the cracks in his research. But he managed to stay in character, acted as if everything was fine, and on the spot answered without missing a beat, "Let me check; I'll call you right back." He changed hats once again to call another department at the bank, this time claiming to be an employee in the wire-transfer room. He obtained the settlement number and called the girl back.

She took the number and said, "Thanks." (Under the circumstances, her thanking him has to be considered highly ironic.)

A few days later Rifkin flew to Switzerland, picked up his cash, and handed over $8 million to a Russian agency for a pile of diamonds. He flew back, passing through U.S. Customs with the stones hidden in a money belt. He had pulled off the biggest bank heist in history – and done it without using a gun, even without a computer. Oddly, his caper eventually made it into the pages of the Guinness Book of World Records in the category of "biggest computer fraud."

Stanley Rifkin had used the art of deception – the skills and techniques that are today called social engineering. Thorough planning and a good gift of gab is all it really took.

Internet Safety

Compiled by Alex Dodwell and Matthew Hagaman in July 2007
Last updated in October 2014

Introduction

The Internet is officially defined as "a worldwide, publicly accessible network of interconnected computers that transmit data by packet switching using the standard Internet Protocol (IP)." While this definition is overly technical, you should know that the Internet is a system for sharing information between computers all over the world. Originally developed for use by the military, by 1985 its use had expanded to the general public. Now people all over the world can use it to share information for business and recreational purposes.

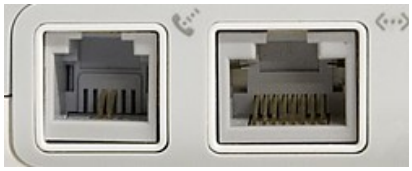
What is the Internet to me?

The Internet is an amazing informational resource. It allows you to connect to and get information from other computers all over the world.

Internet Hardware

The Essentials

The port on the left is found on a **modem**.
The port on the right is found on a **network card**.



Either of these two devices will let your computer talk to other computers over the Internet. A network card is used with high-speed Internet service, to connect to your cable or DSL modem. A modem is used with dial-up Internet service, where your computer is connected to your phone line and to your phone.

Your modem or network card connects you to your ISP (**I**nternet **S**ervice **P**rovider). Your computer will connect to an ISP (generally a company like AOL, AT&T, Comcast, or Frontier) which will connect you to the Internet.

Internet Security

Why is Internet security important?

- Security is a very real problem in the modern world. Billions of dollars are spent every year to prevent and repair damage done by viruses and other security threats.
- With the amount of destructive software floating around on the Internet, any computer that is not properly protected <u>will</u> be compromised.
- This could result in the loss of all of your personal files, and the need to reload all of your software.
- Or worse, it could allow someone to steal your personal information and/or your identity.

Why do computers get viruses and spyware?

- Windows security updates not applied
- No firewall
- No anti-virus software
- Virus definitions not updated
- Opening unfamiliar email attachments
- Clicking "free" offers on pop-up windows
- Peer-to-peer file sharing
- Computer not scanned regularly for viruses or spyware

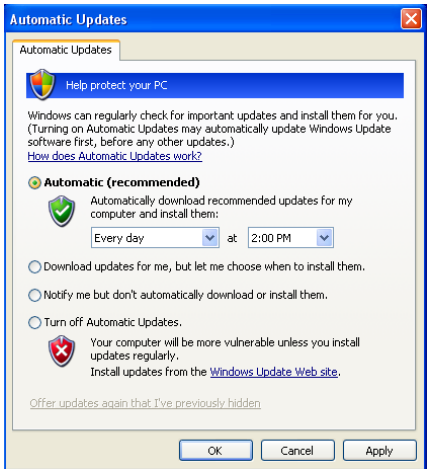
Fortunately, it is easy to keep your computer safe – especially if you develop a weekly routine.

Windows Updates

Windows is a computer program written by humans. Just like any essay or letter you've ever written, it contains mistakes. In Windows these mistakes are called "vulnerabilities." Vulnerabilities occur when a piece of the code that makes up Windows unintentionally allows another program, such as a virus, to make Windows behave improperly.

Microsoft discovers these vulnerabilities through testing or when a large number of computers get affected by a virus. To solve these problems, software updates or "patches" are released that repair the vulnerability so it cannot be exploited anymore.

In order to properly protect your computer you ***must*** check for updates at least once every two weeks or whenever you have to reinstall your operating system.



Downloading Updates

1. Click the "Start" button in the lower left-hand corner of your screen, then "Control Panel", then "Automatic Updates.
2. If you see the dot next to the "Turn *off* Automatic Updates" you will want to change that. For the sake of ease, you can just click the circle next to "Automatic (recommended)" and it will do all the work for you. You can choose when to download and install them by clicking on the drop-down button (arrow button) and choosing how often and what time of day. You can also have the updates automatically download but not install until you choose, or have Microsoft notify you when updates are available and download and install them yourself. Click the "OK" button to confirm any changes.

Firewall

- What is a firewall? Think of your firewall as a very protective security guard and your computer as the club. The security guard controls both what comes into the club, and what gets to leave. You can create a list of programs, computers, etc. that are allowed to access your computer. If something isn't on the list, the firewall will block whatever is requesting access. Common free firewalls include ZoneAlarm, COMODO Personal Firewall, and PC Tools Firewall in addition to the built-in Windows Firewall.

Anti-Virus

- Would you let a surgeon operate on you without washing his or her hands?...of course not.
- By the same token, you never let your computer connect to the Internet without updated anti-virus software running; it's just common sense.
- Without anti-virus software your computer could easily be compromised, and all of your personal files erased, corrupted, or stolen. Some viruses and malware are actually configured to encrypt all of your personal documents, unlocking them only for a fee.

How can I avoid viruses?

- Install one anti-virus program
- Update virus definitions regularly
- Schedule scans at least once every two weeks
- Don't open e-mail attachments from senders you don't know
- Manually scan e-mail for viruses if your program doesn't do so automatically

Nothing is Free

- Everyone likes free stuff, unfortunately on the Internet nothing is really free
- Have you ever seen something like this?→

…Except for viruses

- You will not get a free Best Buy gift card, laptop, iPod, copy of Adobe Photoshop, $1,000,000, etc.
- There is a good chance that you will get a virus
- As tempting as those ads or email offers might seem, clicking them is a bad idea.
- Many file sharing applications (programs that allow people to exchange music and video files illegally over the Internet) such as Kazaa also act like viruses and can render your computer completely unusable
    - These programs are also dangerous because the file you are downloading may contain a virus

…and Anti-virus software

- When selecting your software, there are a LOT of options available to you. Many of them are made by big-name companies that you may have heard of including Symantec and McAfee. These programs are excellent, but expensive and require you to pay annual subscription rates. Fortunately, there are fairly effective, free alternatives. The three most popular are **AVG Anti-Virus** by *Grisoft*, **AntiVir Personal Edition Classic** by *Avira*, and **Avast Home Edition** by *Alwil Software*
    - Don't download an unknown anti-virus program off of the Internet. It may actually be a virus.

Anti-Spyware

- Spyware is a broad category of programs that can easily be installed on your computer without your permission
- Some of these programs just track where you go on the Internet
- Others will change your homepage, create pop-ups, or bring your computer to a virtual standstill

How to Avoid Spyware

- Most of the same rules for avoiding viruses apply to avoiding spyware, but there are a few additional things
- Install two or more anti-spyware programs, including Spybot Search & Destroy, Spyware Blaster, AdAware, Malwarebytes Anti-Malware, or Windows Defender.
- Update the programs on a regular basis
- Scan for spyware once a week
- When installing a free program, read the fine print - some will also install spyware (such as Kazaa or AOL)
- Again avoid all the free Playstation 3, iPod, etc. offers

Anti-Spyware

- There are many options available for free anti-spyware programs. Like free anti-virus programs, they don't offer live technical support. But unlike the anti-virus programs, they offer just as many features and better protection. The problem is that they are a dime a dozen, really. And ironically, if you aren't careful, the program you think is helping you may actually be spyware itself.
- Probably the best set of free anti-spyware programs consists of **Spybot Search & Destroy**, **Malwarebytes Anti-Malware**, and **Windows Defender**. And yes, you will want to install them all. Unlike anti-virus programs, it's okay to have more than one anti-spyware program running on your computer…in fact it's advised.

Spybot

Spybot's immunize function will allow you to proactively block potential spyware threats to your computer. It works with both Internet Explorer and Mozilla Firefox to block threatening pop-ups or sites. To immunize your system, click the green "immunize" cross at the top of the screen. Be sure to do this EVERY time you update the program.

Malwarebytes Anti-Malware

While it is primarily an anti-spyware program, it looks and operates much like an anti-virus program. It should be run and updated weekly to scan for problems.

Windows Defender

As long as Windows Defender has been configured properly (to run a full scan daily and to update definitions before doing so, you should never have to manually use the program, but it is a good idea to check and make sure everything is running properly every month or so. Running the program will immediately tell you the last time the program was updated and the last time a scan was run.

Configure Windows

In this final section of computer protection basics, we will discuss a component of the Windows operating system that is easy to configure and provides an appreciable amount of extra security: ***user accounts***

User Accounts

Whenever you use a computer you are logged in under a user account. There are three types of accounts you can create on a Windows computer.

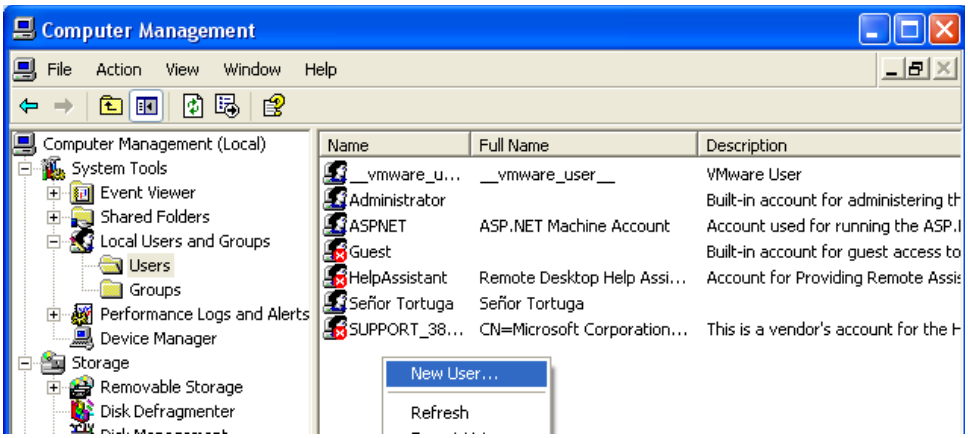
- **Administrators**- An administrator has total freedom to change system settings. An Administrator can view the personal information and files of other users with accounts on the computer, create new user accounts, and modify existing accounts (including removing accounts and changing passwords). An Administrator can install any Windows-compatible software on the computer.

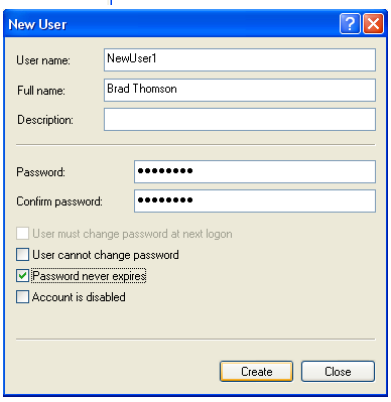
- **Limited Users**- While it is not impossible, it is harder to make irreversible changes to the computer as a limited user. A limited account can run any certified Windows program, and has full control over its own files, but cannot make any changes to system files or to program files. While a limited account provides the most security, it can sometimes be overly restrictive, and prevent someone from performing necessary tasks.

- **Power Users**- Unless you have a good reason to do otherwise, it is best to work while logged into Power User accounts. A Power User can do nearly as much as an Administrator, but with a limited ability to change system settings in ways that could cause harm to the operating system. A Power User can install some kinds of software, but most other applications will require Administrative permissions to install.

  The Power User account option is not enabled by default. In order to create a power user, follow the instructions below.

  - To create a Power User account, first make sure you're logged into the Admin account.
  - Go to "Start" > "Control Panel" > "Administrative Tools" > "Computer Management" and find "Local Users and Groups" on the left. Click the plus, then "Users" and right-click the empty space in the right pane. Create a new user.





- Follow the example on the right (using your own username, Full name, and password).
- After clicking the "Create" button, close the new user window and right-click the new user's name. In the dialog that appears, click the "Member Of" tab and type 'power users'. Click "Check Names" then "OK".

User Account Rules

1. NEVER EVER make the administrator account, which is default, the main user account.
2. Password protect administrator accounts, even the default one, but WRITE EVERTHING DOWN, especially if you put one on the default account. Only by logging in as the default administrator can you delete passwords without having to know them.
3. Create accounts with restricted rights for day-to-day use.
4. Turn off fast user switching and make people log on using CTL+ALT+DEL

How to configure User Accounts

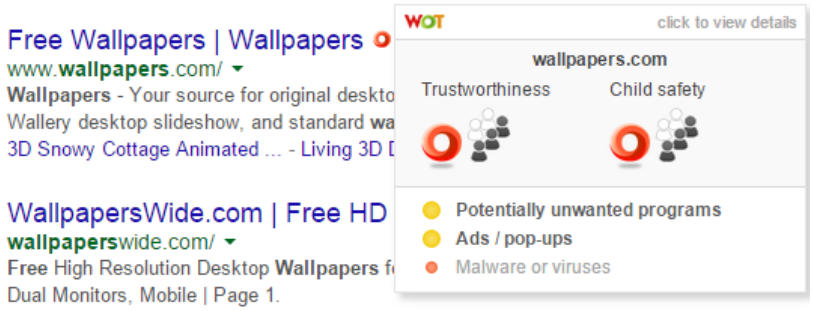
1. Go to "Start" > "Control Panel" > "User Accounts"
2. From this screen, you can change account types, passwords, user icons, and how users log in.

Browsing Safely

- An **Internet Browser** is software application that enables a user to display and interact with text, images, and other information typically located on a website.
- There are two primary browsing programs that you will use on Windows computers…
  - Internet Explorer which is the most popular because it is included with Windows
  - Firefox which can be downloaded for free, and has had relatively few security vulnerabilities
  - Other alternatives like Chrome, Opera, and Safari are known for being both free and secure.

Web Of Trust

Some websites are safer than others. The problem is distinguishing between which ones will allow you to safely download a free educational program, and which ones will give you spyware, unsolicited emails, etc.



One excellent program that will help you distinguish between safe and unsafe sites is Web of Trust.

Web of Trust places a green, yellow, or red icon next to links to different sites. Green sites are the safest

and red ones should probably be avoided.

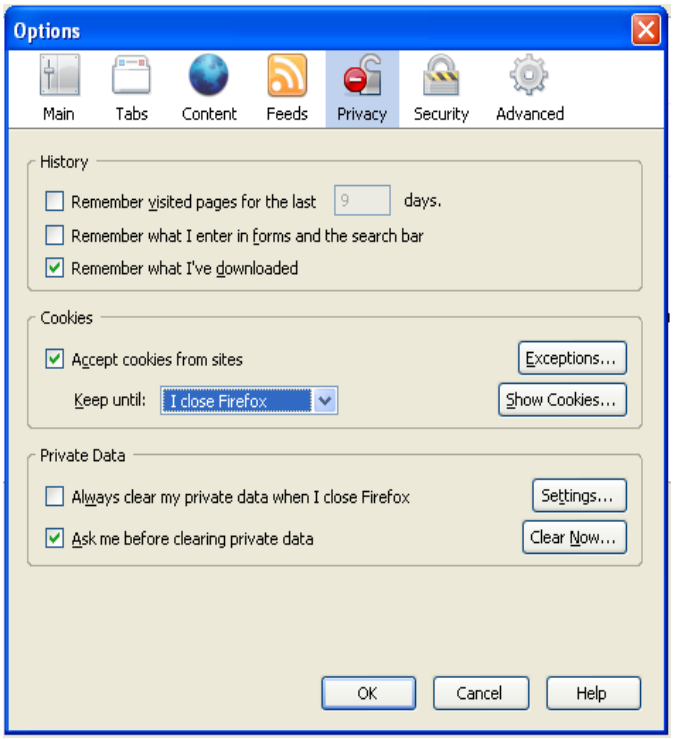
As you can see from this basic Google search, Web of Trust has determined that some of the websites displayed pose a significant risk to your computer. Hovering your mouse over the checkmarks will provide more information about why Web of Trust assigned a website a given score.

Web of Trust is not the only service that offers this information. McAfee Site Advisor is another browser add-on and most anti-virus programs will add a similar feature to your browser.

Cookies

According to Wikipedia, cookies are defined as: “Parcels of information transferred between a server and your web browser for the purposes of authenticating, tracking, and maintaining specific information about your computer activities”

Cookies can be both good and bad. Some of them store password and user information that eases the use of a websites functions.



On the other hand some cookies keep track of your personal information and Internet activities for marketing purposes, display pop-ups on your computer, and are similar to spyware programs.

So what can you do to make sure the “bad cookies” stay off of your computer?

The first thing you can do to control cookies on your computer, is adjust your browser settings
In Firefox select “Tools” and then “Options” from the menu at the top of your browser.

Within the “Options” submenu, select the privacy tab. Then to be on the safe side change the duration that cookies are stored on your computer to “I close Firefox.”

The best thing you can do to prevent malicious cookies from gaining a foothold in your computer system, is regularly running your anti-spyware programs, especially Spybot Search & Destroy. This anti-spyware program looks specifically for cookies that are gathering personal information on you Internet activities.

Advanced Material

The following procedures are things that anyone can do to make their computer more safe and secure, but that many people who regularly use the Internet are not aware of these procedures.

Some of these procedures are somewhat complex and involved, but learning them is a worthwhile investment of time, and can save you quite a bit of grief down the road.

Virus Removal

A virus can be defined as any type of malicious software that causes your computer to do bad things. Despite your best efforts, there is an excellent chance that at some point your computer will get one. But don’t panic. You won’t need to immediately have to wipe and reload your computer. By knowing just a few tricks, you should be able to get your computer (and hopefully your personal files) back up and running in no time.

If the problem is especially severe, you may just want to reinstall the entire operating system. But if there are important unbacked-up files on your computer, you can take the time to remove the virus.

Safe Mode

What is safe mode?

Safe Mode is a special operating mode of Windows that is used when it is having problems running normally. It runs only the bare minimums required to make Windows work. You will not have sound, your screen will not look as pretty, and unless you specify otherwise, you will not be able to connect to the Internet. This is one of the first things you should try to use if your computer won't boot properly, and is absolutely essential to use when removing particularly resistant spyware and viruses. It is best to use the administrator account safe mode, so you have total access to all aspects of Windows.

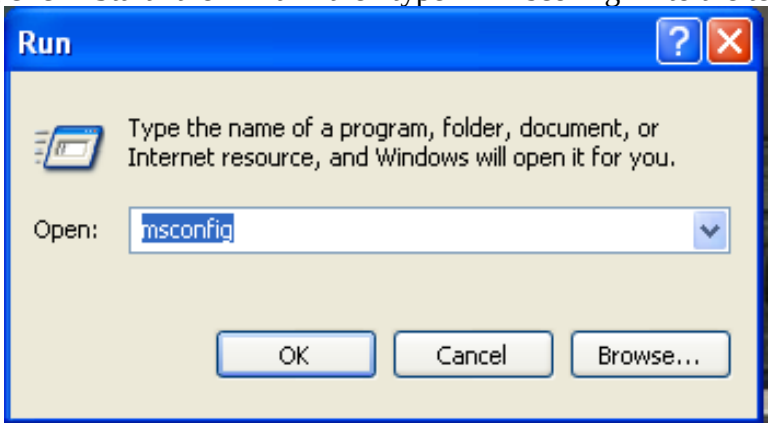
1. Turn on your computer, or restart it if it is already on.
2. BEFORE you see the Windows logo, press the "F8" key on your keyboard. You can press it as soon as the computer's power is on, or as soon as it resets itself (hence the button-mashing). If your computer beeps at you for pressing the key too many times, just ignore it and keep pressing anyway.
3. If you did step 2 correctly, you will be taken to a text-based menu, asking you how you want Windows to boot. Use the up and down keys on the keyboard to choose the option you want. In most cases, just choose "Safe Mode" but if you need network connectivity (don't expect wireless to work), then click "Safe Mode with Networking." If you didn't see the text menu and went right into Windows, you'll just need to restart the computer and try again.

After you have entered safe mode, you should immediately perform a full virus scan. If you restart your computer and are still having problems, move on to the next step.

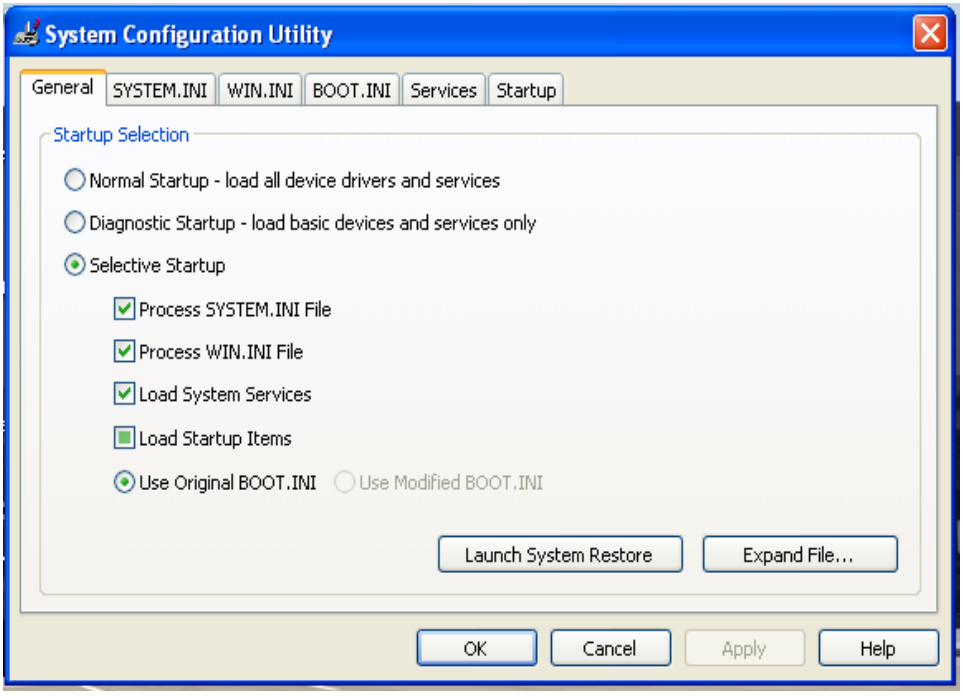
Msconfig

CAUTION!: carelessly playing around with msconfig can cause problems with the normal operations of your system. However, it is important that you know what it is and how it relates to virus and spyware removal. The following will show you how to edit your system files with msconfig and the most common place a virus-associated file will hide.

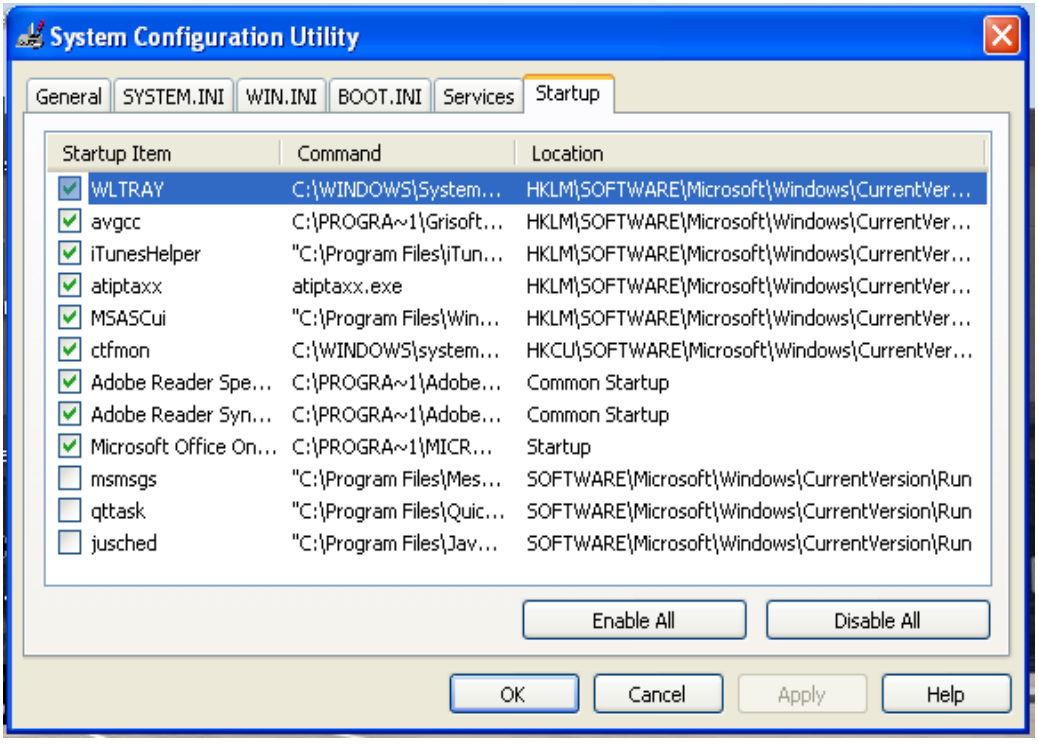
To begin msconfig click "Start" then "Run" then type in "msconfig" into the text box



Initially you will see a screen like the one below. In order to analyze the programs your computer loads at startup click the "Startup" tab.



From here, you can enable or disable any of the programs set to run at startup. Your anti-spyware programs will hopefully eliminate all blatantly harmful entries, but if they fail to solve you programs, you may have to check this section of your computer yourself. For a list of programs frequently found in the startup menu, please see Appendix 1.



Repair Install

This is really one of the last things you can do that doesn't completely wipe out everything on your hard drive. If you've tried everything and you still can't boot Windows from Safe Mode, then a Repair Install may be your last ditch effort.

Of course, it is recommended that you back up your files before you do a Repair Install, which is OK if you can actually get into Windows to back things up. The big difference between a Repair Install and a normal install is that a repair install only repairs Windows. It won't delete programs or files. If Windows gets corrupted by a virus, doing a repair install might restore enough functionality to be able to let you run an anti-virus program.

Should you decide to do one, there is no guarantee Windows will boot. And if it does, it is very important that you don't get online before turning your firewall on. In fact, until you've scanned for viruses, you probably shouldn't connect to the Internet at all.

If this doesn't work, then a complete reinstall may be your only option.

Miscellaneous

Email Solicitations

- Be careful when using email. If you receive an unexpected email from someone you don't know that contains a file attachment, don't open it. The attachment could very well be a virus.
- Equally common are non-virus email scams. Someone will send you a long email detailing how they just inherited a large fortune, or are about to die and bequeath a large fortune, or are involved in a financially lucrative business transaction, etc. Irrespective of what the opening story is, they will always need your help. And "your help" means transferring a sum of money to their account or evening giving them your account information. Unless you want to part with your life savings, I strongly suggest you don't take your supposed benefactor up on the offer.

Always Back Up Your Critical Files

- If there are files on your computer that you cannot afford to lose such as financial records, school reports, etc. <u>always</u> make sure to periodically back them up.
  - Save them to a floppy disk or jump drive
  - If the files are exceptionally important email them to yourself. Why? All the computer security in the world will not help if your house or office burns down and your backups are stored next to the computer.

Password Choices

- When choosing a password make it something easy for you to remember, but not something easy for someone else to guess.
  - Don't make your password your middle name, your birthday, your spouse's name, your address etc.
  - Because it is easy for a hacker to run a "dictionary program" don't make your password a single English word like "squirrel" or "kitty".
- The best passwords are long and contain both upper and lowercase letters, numbers, and special characters. An example would be "Mous3_hunter86" or "L1nco!n52".

The Consequences of Bad Password Choices

- What can happen if you choose an easy password? Maybe nothing. Maybe something very bad.
- Lead singer Chester Bennington of the band Linkin Park used the password "Charlie" for his email account. Someone guessed it and through clever social engineering managed to gain access to all of his personal data, credit card information, phone numbers etc. They used this data to constantly harass and cyber-stalk his family for over 2 years before they were finally caught by the FBI.

Glossary

Adware: Any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.

Cookies: Parcels of information transferred between a server and your web browser for the purposes of authenticating, tracking, and maintaining specific information about your computer activities

Device Driver: A software component used to interact with hardware devices.

Firewall: A hardware or software device designed to control the flow of information to and from a computer or computer network.

File-sharing program: A program used to directly or indirectly transfer files from one computer to another computer over a network. Example: Kazaa, Limewire, Frostwire.

Hardware: The physical part of a computer.

Internet: A worldwide, publicly accessible network of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP).

ISP: An **I**nternet **S**ervice **P**rovider is a business or organization that provides to consumers access to the Internet and related services.

Internet Browser: A software application that enables a user to display and interact with text, images, and other information typically located on the web. Common Internet browsers are Internet Explorer and Mozilla Firefox.

Modem: [from the words **mo**dulate and **dem**odulate] A device that modulates (or changes) an analog carrier signal to encode digital information, and also demodulates such a carrier signal to decode that transmitted information. It does for digital signals what a radio does for radio waves.

Network Card: A piece of computer hardware designed to allow computers to communicate over a computer network.

Packet Switching: a communications process in which packets (units of information) are routed between nodes over data links shared with other traffic. In each network node, packets are queued or buffered, resulting in variable delay.

Safe mode: A diagnostic mode used by the Microsoft operating system. While in safe mode an operating system will have reduced functionality, but it is easier to identify problems because many non-core components are disabled.

Social Engineering: Includes a number of techniques used to manipulate people into divulging confidential information. The term is often used to refer to trickery used to gather personal information or gain access to otherwise secured computer systems. As software gets better at preventing computer vulnerabilities, perhaps the greatest threats to personal security are acts of social engineering.

Software: The computer programs that allow a computer to perform specific functions.

Spyware: Computer software that is installed personal computer to intercept or take partial control over the user's interactions with the computer, without the user's informed consent.

Trojan horse: A program that conceals its true purpose or includes a hidden function a user would not want.

Virus: A computer program that can copy itself and infect a computer without the permission or knowledge of the owner. Once on a computer the viruses usually makes copies of itself that it will distribute to other computers it comes in contact with over the Internet. Many viruses are programmed to damage a computer by deleting files, reformatting the hard disk, or damaging programs.

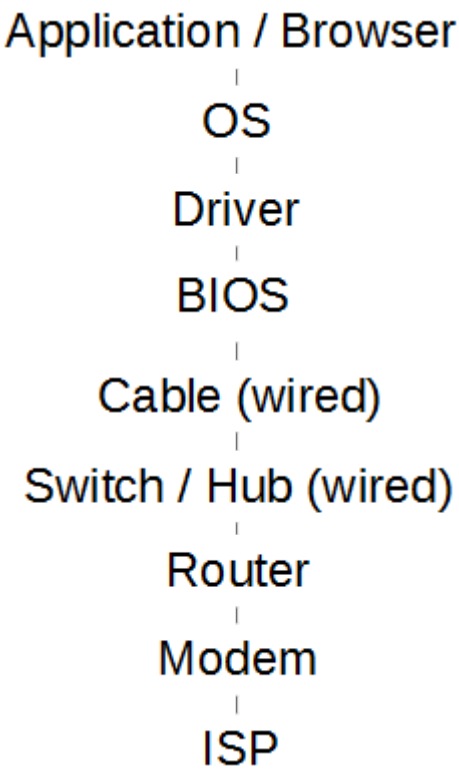
Vulnerabilities: Poorly coded sections of programs that be exploited by hackers to illegally gain access to computer systems.

Appendix 1 (MSConfig Decoded)

acroTray	Adobe Acrobat Speed Loader	Allows Adobe Acrobat Reader and related services to load more quickly	May be removed to speed up system
Adobe Reader Speed Loader	Adobe Reader Speed Loader	Allows Adobe Acrobat Reader and related services to load more quickly	May be removed to speed up system
atiptaxx	ATI Graphics Utility	Driver that links your video card to the operating system	Do not modify
avgas	AVG AntiSpyware	Spyware removal tool	Do not modify
avgcc	AVG Antivirus	Anti-virus program	Do not modify
ccApp	Symantec Antivirus	Auto-protect service provides realtime protection against viruses as they are downloaded or inserted on disc.	Do not modify
ctfmon	**Microsoft Office Component	**Interfaces Microsoft Office with Text & Speech Components	**May be removed to speed up system
hkcmd	Intel Graphics Driver	Provides User Interface for Intel Integrated Graphics	Do not modify
igfxpers	Intel Graphics Driver	Module loaded to help Intel Integrated Graphics to function	May be removed to speed up system
igfxtray	Intel Graphics Driver	Allows Intel Integrated Graphics to function	Do not modify
Issch	Install Shield Update Service	Checks for updates to Install Shield, a software package installer	May be removed to speed up system
isuspm	Install Shield Update Service	Checks for updates to Install Shield, a software package installer	May be removed to speed up system
jusched	Java Update Scheduler	Checks for updates to Java, a program that is required to access some rich Internet content.	May be removed to speed up system, but be sure to manually check sun.com/java for updates periodically.
MSASCui	Microsoft Windows Defender	Provides the user interface for Windows Defender (spyware removal tool)	Do not modify
msmsgs	Windows Messenger	An instant messaging system built into windows	Tools > Options > Preferences “Run Windows Messenger when Windows Starts”
nvmctray	nVidia Graphics Utility	Enables the nVidia options in the system tray	May be removed in Control Panel > nVidia Control Panel
qttask	QuickTime Taskbar Utility	Allows QuickTime and iTunes to load more quickly	May be removed to speed up system through the QuickTime Control Panel Module (Advanced tab, uncheck “Install QuickTime Icon in System Tray”.
VPTray	Symantec Antivirus	Provides user interface for Symantec Antivirus (virus protection tool)	Do not modify

** Ctfmon has been known to be used as a disguise point for viruses and spyware. The legitimate service can be disabled by navigating to Control Panel > Text & Speech Services.

Network Troubleshooting Guide



There are many levels at which you might identify a problem with your network connection, but we will explore the most likely areas of concern.

Wired Networking

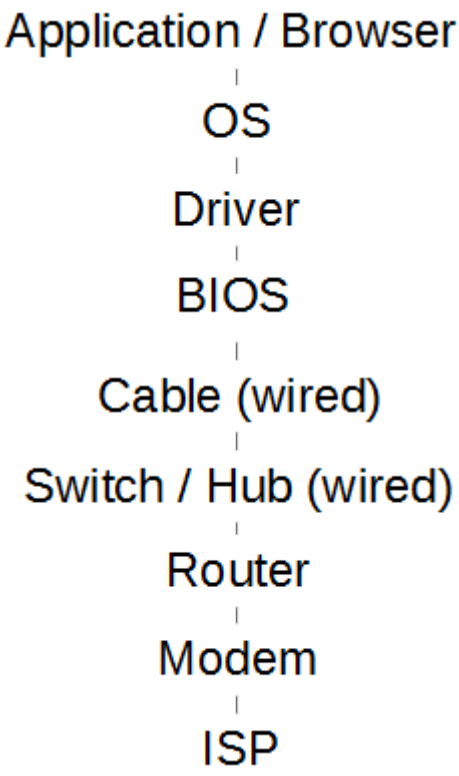
1. Reset network adapters. In Windows Vista or later, this is part of Windows' built-in troubleshooter: right-click the networking icon and select troubleshoot (if there is a red X on this icon, jump forward to step 3). In Windows XP and earlier, you will need to browse to Start > Control Panel > Network Connections, select the network device in use, and right-click > disable. Wait a moment and then right-click > enable.
2. Restart the PC. Many temporary problems are avoided by turning the computer off and on again. When you have restarted the computer, open the command prompt and type `ipconfig` and enter. This will show you your computer's IP address and gateway. An IP address starting in 169.254.x.x indicates that Windows cannot configure itself – check connectivity settings. Also in command prompt you can perform a series of pings (`ping google.com` or `ping 8.8.8.8` to see if you truly have Internet access and `ping [gateway address printed from ipconfig]` to see if you can communicate within the network.
3. Restart the switch / router / modem. Problems occasionally occur where the device that connects your computer a network has a problem. Resetting this(these) device(s) by powering it off and on again can sometimes resolve an intermittent problem.
4. Check the firewall. Most software firewall systems have “block all” modes, which would prevent any and all network communication. Beyond the “block all” mode, firewalls are often the culprit when you are having trouble accessing a specific type of resource (IM or FTP versus browsing the web). At this point it may also be useful to try using a different browser and/or checking the BIOS to ensure the network adapter you are using is enabled.
5. Use a Linux Live CD / DVD. If you can boot from a Linux Live CD / DVD and access the Internet, there is a problem at the operating system level – perhaps a virus or malware. Proceed to 6a. If you still cannot access the Internet, it is time to call your Internet Service Provider. Proceed to 6b.

6a. Conduct a Virus Scan. Viruses and other malware sometimes block Internet connectivity as part of their (dys)functionality. Boot your computer into Safe Mode – press the F8 key rapidly between the BIOS POST screen and the Windows boot screen and run a virus scan from this environment. Safe mode prevents the malware from starting and makes it easier to find and fix.

6b. Call Your Internet Service Provider for help.

7. Start Replacing Hardware. Your Internet Service Provider should be able to help you identify if there is a problem with your hardware or if there was trouble on their end. As a last resort, you can try replacing different pieces of hardware with known working hardware: start with the modem, then router, then switch (these are sometimes combined), cable, and network card.

Network Troubleshooting Guide



Wireless Networking

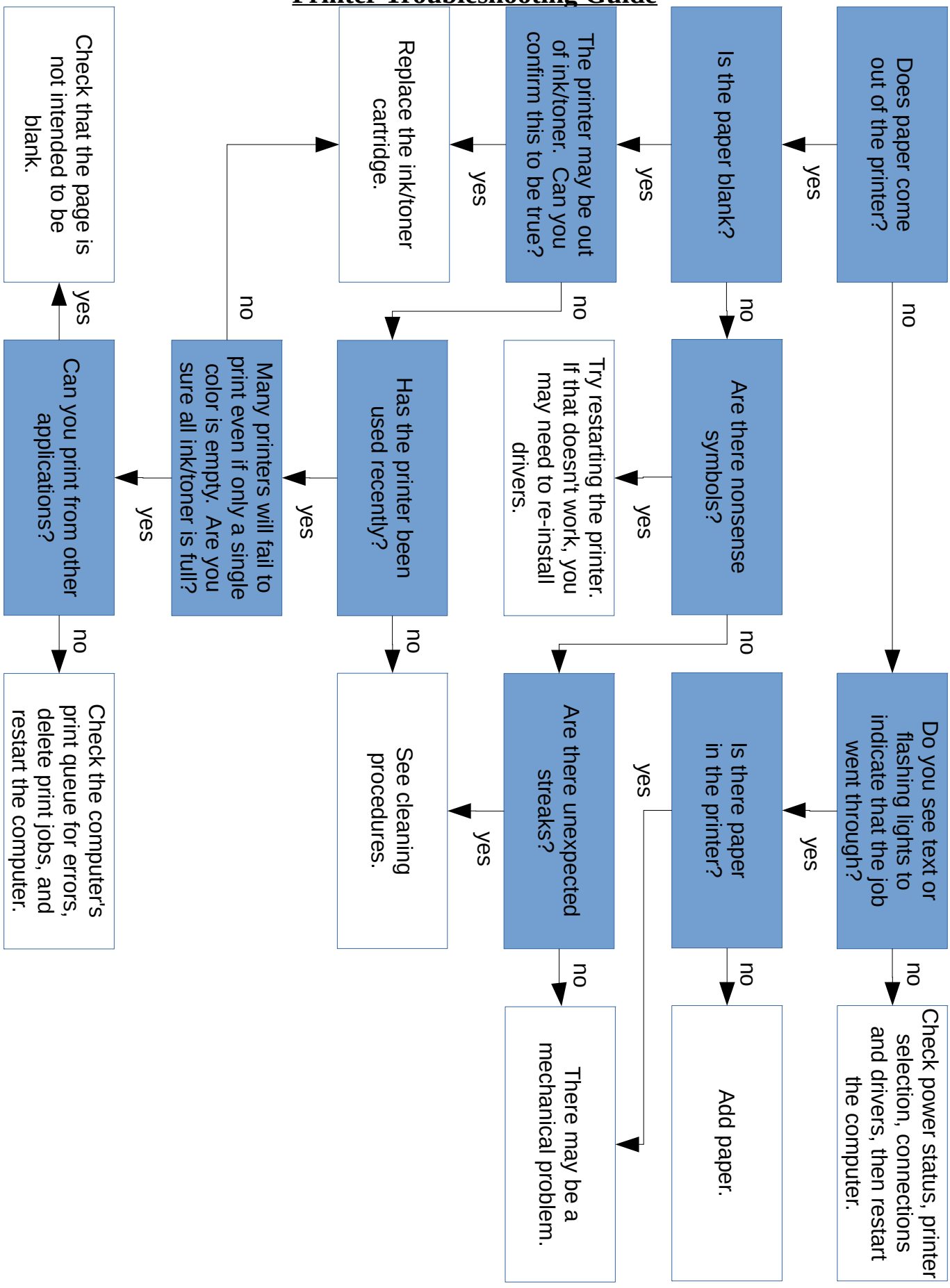
1. Reset network adapters. In Windows Vista or later, this is part of Windows' built-in troubleshooter: right-click the networking icon and select troubleshoot (if there is a red X on this icon, jump forward to step 3). In Windows XP and earlier, you will need to browse to Start > Control Panel > Network Connections, select the network device in use, and right-click > disable. Wait a moment and then right-click > enable.
2. Restart the PC. Many temporary problems are avoided by turning the computer off and on again. When you have restarted the computer, open the command prompt and type `ipconfig` and enter. This will show you your computer's IP address and gateway. An IP address starting in 169.254.x.x indicates that Windows cannot configure itself – go to step 5. Also in command prompt you can perform a series of pings (`ping google.com` or `ping 8.8.8.8` to see if you truly have Internet access and `ping [gateway address printed from ipconfig]` to see if you can communicate within the network.
3. Restart the switch / router / modem. Problems occasionally occur where the device that connects your computer a network has a problem. Resetting this(these) device(s) by powering it off and on again can sometimes resolve an intermittent problem.
4. Switch to wires. Try hooking your computer up directly to the switch / router / modem. If this works, the problem is related only to wireless connectivity and either the router, network adapter, or wireless settings are at fault.
5. Check wireless settings. Does your computer see the wireless network? Is the passcode correct?
6. Check the firewall. Most software firewall systems have “block all” modes, which would prevent any and all network communication. Beyond the “block all” mode, firewalls are often the culprit when you are having trouble accessing a specific type of resource (IM or FTP versus browsing the web). At this point it may also be useful to try using a different browser and/or checking the BIOS to ensure the network adapter you are using is enabled.
7. Use a Linux Live CD / DVD. If you can boot from a Linux Live CD / DVD and access the Internet, there is a problem at the operating system level – perhaps a virus or malware. Proceed to 8a. If you still cannot access the Internet, it is time to call your Internet Service Provider. Proceed to 8b.

8a. Conduct a Virus Scan. Viruses and other malware sometimes block Internet connectivity as part of their (dys)functionality. Boot your computer into Safe Mode – press the F8 key rapidly between the BIOS POST screen and the Windows boot screen and run a virus scan from this environment. Safe mode prevents the malware from starting and makes it easier to find and fix.

8b. Call Your Internet Service Provider for help.

9. Start Replacing Hardware. Your Internet Service Provider should be able to help you identify if there is a problem with your hardware or if there was trouble on their end. As a last resort, you can try replacing different pieces of hardware with known working hardware: start with the modem, then router, then switch (these are sometimes combined), cable, and network card.

Printer Troubleshooting Guide



Printer Troubleshooting Guide

Checking Connections

If the printer is connected to a network rather than directly to a computer, refer to the *Network Troubleshooting Guides* (pages 45-46). If the printer is connected directly to the computer, check that both ends are firmly secured, then proceed to checking drivers.

Checking Drivers

To see all printers installed on a Windows computer, browse to Start > Control Panel > Printers or Start > Control Panel > Devices and Printers. Ensure that the printer you want to use is listed, and check its status. If the printer is listed, you may find useful error information or the printer may have a positive status of Idle or Ready. If the printer is listed as offline, check the computer and printer's connections.

If all else fails, it may be worth downloading the latest drivers from the manufacturer's web site and installing them.

Cleaning Procedures

Inkjet printers can sometimes have clogged printer heads, especially if they have not been used for a period of time. These can often be cleaned using a little rubbing alcohol and a few cotton swabs. See your printer's manual for instructions.

Laser printers may occasionally benefit from a gentle vacuuming of excess toner both inside and outside of the printer (without attachments coming in contact with any printer parts), or belt and/or drum units may need cleaning (often with a vacuum or rubbing alcohol on a soft rag). See your printer's manual for instructions.

Mechanical Problems

Mechanical problems are beyond the scope of this guide. See your printer's manual for instructions.

Replace Ink / Toner

Ink and Toner are often best replaced as a whole unit, but it can sometimes be more economical to refill ink / toner using refill kits. See your printer's manual for instructions.

Restarting the Printer

Many printers retain memory and power even after they are turned off. To completely power off the printer, use its power button and wait for power to cycle off. Then unplug the power cable, wait 25 seconds, and plug the cable back in. Consider clearing the computer's print queue and/or restarting the computer, then power the printer back on.

Selecting a Printer

Many computers have access to more than one printer, and modern computers often have virtual printers as well. Ensure that you have selected the printer you intend to use in the application's print dialog box or close the program, set the printer as the default printer, re-open the program, and try printing again.

Setting a Default Printer

To see all printers installed on a Windows computer, browse to Start > Control Panel > Printers or Start > Control Panel > Devices and Printers. Right-click the printer you wish to use as the default device and select Set as Default.

The Print Queue

The print queue is the line of print jobs in progress. If there is a problem, errors will often appear here. To open the queue, double-click the printer icon in the computer's system tray (just to the left of the clock in the bottom right-hand corner of the screen). You can usually delete erroneous jobs by right-clicking the job and choosing cancel, though you may need to do this more than once. Restarting the computer is recommended.

Video Troubleshooting Guide

This guide applies to external monitors only.

1. Check cables. In order for video to travel along the data cable, it must be secured on both ends. Most monitor cables screw into their ports to ensure they stay in place. Equally important is the power cable – if the power cable has come loose, secure that as well.
2. Secondary source. If video from one device does not work, does video from a different device? If a secondary source produces video, proceed to 3a. If it does not, proceed to 3b.

3a. Check display settings. Boot your computer into safe mode (press the F8 key rapidly between the BIOS POST screen and the Windows boot screen). You should have video both during the POST and in safe mode. Check the display settings in Control Panel to verify they are correct. Ensure you have selected a low resolution (i.e. 1024x768) and that the refresh rate is supported by your hardware.

3b. Secondary monitor. Try hooking the computer up to a different monitor.

4. Check alternate ports / BIOS settings. If your system has more than one monitor port, try using a different one. Integrated / on-board and distinct video cards sometimes fight with one working and the other not. If this is the case, you can use the second port or change BIOS settings to ensure the proper port is being used.
4. Secondary video card. There could be a problem with the on-board or distinct video card. If the video card is integrated into the motherboard, check for bloated or leaking capacitors – it could be the end of your motherboard. Either way, hooking up a new video card is a good way to test the problem further.