Practical and Simple Tips to Help You Avoid Common Computer Disasters

The following tips will help you avoid common computer disasters. Like many preventative measures, you may never know the trouble you are saving yourself if you follow them. It is intended for average users, not for "power users," who often have other, better, solutions.

The main point is simple: There really is no such thing as unprotected safe computing any more. The internet, in particular, is becoming especially dangerous. You must actively take steps to protect yourself.

The text on each subject below is pretty brief. There is an abundance of help on the web about all of these subjects if you need more explanation. The document is divided into two sections, the first, on general security, email, and the internet. Following that is a shorter section about your personal files.

GENERAL SECURITY, EMAIL AND THE INTERNET

Passwords and User IDs

For each computer or online service you use, you should have a user ID and password. Commit your password to memory and don't share it with anyone. Easily-identifiable items should be avoided when creating passwords:

- Your birth date or a family member's birth date
- Names of family members or pets
- Social Security number
- Phone numbers
- Dates of important events, such as anniversaries

Tips for creating strong passwords:

- Use a combination of numbers, letters and special characters (for example, @, !, #, etc.)
- Longer passwords are better
- Make sure it's something you can remember without writing it down

Patches: Keep Your Software Up-to-date

Most software makers provide free "patches" (a small program made to fix various problems in their software) that you can download from their Web site. It's a good idea to check periodically for these patches and install them, especially if it is a Microsoft product or the application accesses the internet. If both (like Internet Explorer, Outlook, Media Player, or Windows), check often. Virus writers, hackers, and other ne'er-do-wells target Microsoft products, simply because so many people use them.

Browsing: Consider Using Something Other than Microsoft Internet Explorer

For the past few years (this was written in early 2005) it has become apparent that Internet Explorer is a target for people trying to hack into, drop "spyware" (more on this below) on to, or otherwise try and harm, your computer. You have to believe that as soon as Microsoft releases a new security patch, these villains are figuring out ways to get around or through them. Point? Try switching to a different browser. One that is increasingly popular (and my favorite) is Firefox. It's free, easy to use, and can be found at <http://www.mozilla.org/products/firefox/>.

Phishing: Email Scams

Phishing involves the use of email messages that appear to come from your bank or another trusted business, but are actually from imposters. These emails typically ask you to click a link to visit a Web site, where you're asked to enter or confirm personal financial information such as your account numbers, passwords, Social Security number or other data. Although these Web sites may appear legitimate, they are not. Common examples in the past few years include Ebay, PayPal, and Yahoo, but there are more (I, for example, have been getting them from Washington Mutual Bank for about 6 weeks now). Thieves can collect whatever data you enter and use it to access your personal accounts. Look for these warning signs of phishing:

Language and Tone. The email may urge you to act quickly by suggesting that your account is threatened. It may say that if you fail to update, verify or confirm your personal or account information, access to your accounts will be suspended. The wording may also be sloppy and contain misspellings.

Requests for Personal Information. Scam emails typically ask for personal or account information such as:

- Account numbers
- Credit and check card numbers
- Social Security numbers
- Online banking user IDs and passwords
- Mother's maiden name
- Date of birth
- Other confidential information

Non-secure Web Pages. Clever thieves can build a fake Web site that looks nearly identical to an authentic one. Watch out for *non-secure* Web pages that ask for sensitive information: *Secure* sites will typically display a lock in the status bar at the bottom of your browser window.

Here are some safety tips to decrease the risk of being a phishing victim

Be Suspicious of Demanding Messages. Messages threatening to terminate or suspend your account without your quick response should be treated as suspicious. A legitimate bank or business should not request personal information from you over an unsecured Web site. When in doubt, call the business' customer service number (available on your account statement) to confirm the status of your account. Do not use telephone numbers found on the suspected Web site.

Always Type in the URL of the Web Page You Need. Phishing scams rely on embedded links that take you to fake Web sites. It's safer to type your bank's Web address directly into your browser so you know you're visiting the legitimate site.

Reducing and Avoiding Spam

For those who don't know what the term means, Spam is simply unsolicited email. The following are suggestions for reducing the amount of spam you get (understanding that the only way to completely eliminate spam is to stop using email).

Never Post Your Real Email Address on Forums, Bulletin Boards, Chat Rooms, Web Page, Etc. Spammers use special programs which "harvest" these and use them to build spam lists. Once your email address has been "caught" in this way, you'll never got off the spammers' lists. Alternatively, there are ways to "disguise" your email address in chat rooms, web pages, etc.

Consider Using Fake Email Addresses When You Sign up for Things on the Web. If you must "register" to gain access to a web site (and anymore, I just don't bother most of the time, on principle), use a fake email address if you can. Obviously, if you need to receive email from the site (for example, a transaction) this doesn't apply, but the idea is simple: Don't give your email address out unless you have to. An exception to this is a site that you trust explicitly. At minimum, they should be a large, reputable company, and have a privacy policy that clearly states they won't sell your email address.

Watch out for Those Check Boxes. If you do use your real email address when you sign up for something on the Web, there is often some innocent-looking text at the end of the form saying something like: "YES, I want to be contacted by select third parties concerning products I might be interested in." Quite often, the checkbox next to that text is already checked and your email address will then be sold to any number of people and companies. So, uncheck the box!

Never, Ever, Click a Link in an Email Which Invites You to "Unsubscribe." You probably got the spam as a result of the spammer sending a message to hundreds of thousands of random addresses. Clicking that link tells the spammers that the email account is active. This means you will get more – a lot more – spam. Similarly, do not ever respond to spam email, for the same reason.

Set up Multiple Email Addresses. If you regularly sign up to a lot of web sites, consider having one email address just for this purpose, while keeping your main email address private to friends and family.

Makes Use of Filters or "Rules." In Yahoo they are called "filters"; in Outlook they are called "rules." In either case, you are telling your email program that if certain words or phrases (which you specify) are found in the email, the email should be automatically delivered to your trash folder. For example, using a "Viagra" filter last year, I am sure, saved me from seeing hundreds of spam emails.

Install and Use a Firewall

Before you connect your computer to the Internet, you should install a firewall. If you are using a broadband connection (DSL or cable modem), definitely; if only a telephone (regular) modem, perhaps not.

A firewall can be thought of as a security guard for your home computer. The guard is a piece of software that helps protect your computer against hackers and many computer viruses and worms. A firewall lets you define which connections between your computer and other computers on the Internet are allowed and which are denied. There are several free firewall programs available that provide the capabilities you need to help make your home computer more secure. I use Zone Alarm, available at <http://www.zonelabs.com/>. Windows XP has firewall built into it, but I know little about it (I don't use XP – sorry).

Eliminate Pop-ups Ads While Browsing

If you use Firefox, you probably don't have a problem with pop-ups. Or, you may have a toolbar or something else that stops them. In the event pests are still getting in the way of your browsing life, try Popup Stopper (it's free), available at <http://panicware.com>.

Spyware and Adware

Spyware and adware are not necessarily the same thing, but for our purpose we will treat it as such. Many free utilities that you download from the Internet will install hidden software that send details of the websites you visit and other information from your computer (which can include your email address) to advertisers so they can target you with popup ads and spam. They also reduce performance of your computer, and can often delete files and do other malicious things (technically, this latter type is called "malware"). The first step to protect yourself? If and when you install shareware, read the legal screens carefully and see if they are installing anything other than what you expected.

Next, you should have the following free applications installed on your computer:

- Ad Aware, available at <http://www.lavasoftusa.com/software/adaware/>
- Spy Bot Search & Destroy, available at <http://www.safer-networking.org/en/index.html>

Run each program every few weeks. And, before you run it, check for updates. (Remember security rule number 1: As soon as we figure out a new way to stop "them," "they" are hard at work finding a way around it!).

Viruses & Worms: E-mail Attachments

Email viruses and worms are fairly common. There are several steps to guard against them. The first, and most important rule: Never, never, never, double-click a file to open it! Ever. If you need it, save it to your hard disk first (usually by right-clicking and selecting "save as"). Then scan it with virus software.

Next, never download or open attachments with the following extensions (the letters that come after the period in the filename):

- .PIF
- .BAS
- .EXE
- .SCR
- .VBS

Here are some steps you can take to help you decide what to do with email message attachments. As a rule, you should only open and read a message that passes all of these tests:

- Is the email from someone you know? Have you received email from this person before?
- Were you expecting email with an attachment from this sender?
- Does the email subject make sense based on who is sending the e-mail? Would you expect this type of attachment from this person?

Finally, to be really safe, consider using a free web-mail service for all of your email (Yahoo, for example, allows you to pick up email from other email accounts). Why? First, if you do get a virus in an email, it's on *their* computer (unless you download it). Second, they usually have anti-virus programs they use to screen your email – you don't have to do anything. And, their anti-virus software is always up to date!

How to Avoid Viruses

Viruses can infect a home computer in many ways: Through floppy disks, CDs, e-mail, Web sites and downloaded files. If your computer starts doing very strange things, suspect virus right away and take steps to check and correct.

Anti-virus programs help protect your computer against most viruses, worms, Trojans and other unwanted invaders that can make your computer “sick.” Viruses, worms and the like often perform malicious acts, such as deleting files, accessing personal data or using your computer to attack other computers. If a file is found to be infected with a virus, most anti-virus programs provide you with options of how to respond, such as removing the harmful item or deleting the file. Installing an anti-virus program and keeping it up-to-date is the best defense for your home computer.

So, install and use an anti-virus program. It’s worth the money. Easilly as important, update the “virus definitions” (the database the program uses to look for viruses) frequently. New viruses are being written constantly, and the program can only detect the ones it knows about.

In addition, I also make use of one of several free virus-checking site on the web that scan your computer over the internet. Try, for example,

- Trend Micro: <http://housecall.trendmicro.com/>
- Tech 24 (Macafee or Norton): <http://www.tech24.com/virusscan.asp>
- PandaSoft: <http://www.pandasoftware.com/activescan/>

Final tips for avoiding viruses:

- If a friend wants to put a floppy disk (or flash drive) in your machine, scan it first
- If *you* have a disk (or flash drive) that has been in another computer (especially in a common computing environment, like university computer labs), scan it before you use it in your computer again
- Avoid MS Word documents on the Internet

YOUR PERSONAL FILES

Backup Your Data Early and Often

It is a good practice to have a strategy to back up files and folders on your computer. To say this in a simpler way, you should always have two copies of all of your data files.

Some elements of a good backup strategy include:

- Backup your files often (I do it at least once a week – it’s worth the trouble!)
- It is also important to know and understand the location (the directory, or folder) of your files. You can’t back them up if you don’t know where they are. I usually create a separate directory – not “My Documents” – where I store all my files.
- Backup to a separate physical disks: A remote server, via FTP, a CD-ROM, another hard disk on your computer, or another computer on a network.

However you do it, there will come a day when you are relieved that you have done so. I promise.

Floppy Drives are Out

No one needs to, or should be, using floppy disks these days. The best and safest choice for primary data storage is your hard disk. The idea that hard drives are unreliable is about 10 (or more) years out of date.

To transport files, buy a flash drive (or jump drive). These cost anywhere from $20 to $50 (depending on the size) and plug into your USB port (almost all computers have these now). They are smaller, hold more data (lots more), and don't break!

If you must use floppy drives, use good quality disks. And, if the disk is old, or even slightly defective, transfer the files to a new one and discard the old. It's just not worth the risk!

Make Sure Your Data Are Portable or Transferable

If you use an esoteric word processor (for example, MS Works, Lotus), it's probably a good idea to have second copies of important files saved in another, more common file format (like Word), in case your computer goes down. Most people won't have these applications, so if you need to access your data in an emergency, you won't be able to unless you have another version.