
Computer Help, Tips & Advice From The Experts!

Special Report

Brought to you by:
[How To Buy A Laptop.com](http://HowToBuyALaptop.com)

Welcome!

This is a free ebook. You are welcome to share this ebook with your friends, website visitors and ezine subscribers. The only restriction is that you cannot modify the ebook in any way.

Disclaimer

The author and publisher of this report have used their best endeavors in preparing the information.

All articles contained herein have been sourced from online article directories where articles are submitted expressly for the purpose of royalty-free distribution. The original copyright of each article remains with the article's author.

The authors and publisher do not warrant the performance or effectiveness of the websites listed in this information, nor can they warrant the applicability of any of the material to an individual circumstance.

The authors and publisher shall in no event be held liable for any loss or damages caused. As always, the advice of a competent legal, tax, accounting or other professional should be sought. This report is not intended as a source of legal, accounting, business or financial advice, but is provided for informational purposes only.

Table of Contents

10 tips to Stay Safe and Secure Online	4
5 Tips For Buying The Right Laptop Computer.....	6
2 PC Annoyances and How To Solve Them!.....	8
How To Keep Your Computer Virus Free	10
Internet Safety.....	12
Beginner's Guide to Music File Formats	14
5 Ways to Speed Up Your PC	16
The Seven Golden Rules Of Data Backups.....	18

10 tips to Stay Safe and Secure Online

by Steve Robson

The Internet can be a dangerous place.

While you're enjoying the convenience of online shopping, Internet banking and subscription websites, nasty people lurk around every corner.

Hackers, fraudsters, identity thieves and many others would love to get hold of your personal details.

And what stands between you and a security disaster?

Your password.

Just 8 little characters long, it's your last line of defense online. So here are 10 tips for choosing and using bullet-proof passwords that will protect you from harm:

Tip 1 - Avoid the obvious

Passwords based on personal details are too easy to guess. Avoid using names, places, favorite sports teams, or "password".

Tip 2 - Make it non-dictionary

One option a thief might try to crack your password is a brute-force dictionary attack. So choose something that you won't find in any dictionary.

Tip 3 - Use the full 8 characters

The more characters a password contains the more secure it becomes, so fill that password field to the max.

Tip 4 - Mix the case

Deter thieves further by using a combination of upper and lower-case letters. A mIXeD cAsE password adds another layer of protection and is ever harder to guess.

Tip 5 - Include non-alphabetic characters

Adding numbers and non-alphabetic characters (like a hyphen) to your password makes it less likely to be cracked than something purely alphabetic.

Tip 6 - Don't write it down

This should be obvious but it's amazing how many scraps of paper surround the world's PCs.

Tip 7 - Assign a different password to each login id

If thieves get hold of your password, they'll try it in every online system available. Use a separate password at each website and you won't have all your eggs in one basket.

Tip 8 - Employ a password manager

Remembering multiple secure passwords can be challenging. Specialist software like <http://www.robo-form.com> manages your passwords securely and automates the login process.

Tip 9 - Logout when you're done

Always hit the logout button when you've finished using a secure site like online banking.

Tip 10 - Close that browser

Web pages and passwords can be cached in the browser, so close down your browser window for added security.

Follow these simple common-sense tips and you'll enjoy greater online security while benefiting from the many advantages the Internet has brought.

About the author:

Steve Robson is a successful technical author and contributor to 'How To Buy A Laptop.com' - the definitive online guide for buying a laptop computer.

Check out: <http://HowToBuyALaptop.com>

5 Tips For Buying The Right Laptop Computer

by John San Filippo

It's easy to be intimidated by all the laptop models on the market today. There are literally dozens and dozens in every price range.

The key to finding the right one for you is to step back and consider exactly how you plan to use your laptop. When you define what you need before you go shopping, buying the right machine becomes much easier.

Here are 5 basic factors to consider:

1. Size

In the world of mobile computing, size definitely matters. The size of a laptop affects two key areas: portability and display size.

If you're always on the go and will be using your computer only in short bursts, a so-called ultralight will save you some shoulder strain. On the other hand, if you're going to spend hours in front of your laptop, a larger display may be in order.

Today, some laptop displays exceed 17 inches, rivaling the display size of many desktop systems. The down side is that these monsters can easily weigh three times as much as an ultralight.

2. Hard Drive

Speaking of size, what about the size of the hard drive? One way to approach this issue is to ask yourself the following question: Will this be my primary computer, or will it supplement my desktop system?

If the former, you should look for a bigger hard drive - 60 GB or more. If the latter, you may be able to make it with a 20-30 GB hard drive.

But even this isn't absolute.

If, for example, you plan to copy a huge MP3 library from your desktop system to your laptop to make your music library portable, you'd be well advised to err on the side of too big.

3. Memory

In determining the right amount of system memory, or RAM, take a look at the ways in which you intend to use your laptop:

If your needs are somewhat mundane - email, spreadsheets, word processing, etc. - 256 MB of RAM should be plenty. This is a common configuration for many laptops, so it means you probably won't need to spend extra for more RAM.

On the flip side, if you're an aspiring mobile digital photographer or videographer, you should stuff your laptop with as much RAM as it can hold.

In fact, exactly how much RAM your laptop can hold may in part drive your purchase decision. Applications for editing and manipulating multimedia content are notorious resource hogs.

4. Network Connections

Thanks in no small part to the Internet, computing in the 21st century relies heavily on being connected:

Connected to the Internet, connected to a corporate network, connected to a wireless network, connected to a home network, connected to an online service.

Your life will be easier if you buy a laptop that includes built-in means to connect to them all.

5. Price

If you're considering a laptop, you're probably wondering how much money you'll need to spend.

A few years ago, you'd be hard-pressed to find one for under \$2,000. Today, there are plenty of laptops to be had for under \$1,000.

What's more, most of the major manufacturers offer a variety of financing options.

Laptop prices have come down, to be sure. However, a laptop still represents a fairly major purchase for most people. If you take the time to search for a laptop that meets your specific needs, you should get many years of use and enjoyment from this important investment.

About the author:

The author, computer journalist John San Filippo, has created the definitive guide for buying a laptop computer at: www.HowToBuyALaptop.com

2 PC Annoyances and How To Solve Them!

by Jim Edwards

I have a love-hate relationship with my computer.

In fact, often I love to hate my computer!

It will do things I know even the great Mr. Gates didn't intend, and it usually does them at the least convenient time (like when I'm on a deadline or in a hurry).

Rather than the usual whining and doing nothing about it, I've decided to share a couple of things that previously annoyed the heck out of me and the solutions I found to help you avoid these same problems.

Disappearing Internet Explorer Status Bar

The status bar at the bottom of the Internet Explorer web browser serves many purposes.

It allows you to hold your mouse over a link to see where the link will take you.

It enables you to see a page's loading progress as you wait for it to download.

Most importantly, the status bar allows you to see the little gold "lock" symbol that lets you know you've made a connection to a secure server (very important to know before you input credit card data).

For some inexplicable reason, from time to time, this status bar disappears from my browser.

Also, the toolbars at the top tend to move periodically and mess up my "system" for surfing the Internet.

Now, it's not the end of the world, but it really ticks me off when things change and I didn't change them! If this ever happens to you, here's how to literally "lock" the toolbars and status bar in place so they don't disappear or move again.

First, close all your Internet Explorer web browser windows except for one. If the status bar doesn't already appear in the window, go to "View" and then click "status bar."

Also, make sure you have all the toolbars arranged the way you want them.

Next, place your mouse over a blank spot on one of the tool bars at the top of the Internet Explorer browser window.

Right-mouse-click and a menu will appear where you should check the option "Lock the Toolbars."

Then, while holding down the <Ctrl> key, click the "X" in the upper right corner of the window to close it. This will set your selection.

If you ever need to change your toolbars in the future, simply right-mouse-click on the toolbar and uncheck the "Lock the Toolbars" option, make the changes, and then re- lock the toolbars to keep them from moving or disappearing.

Missing File Extensions

One of the biggest pains in the neck involves opening Windows Explorer, viewing a list of files, and not being able to see the file extension (.doc, .txt, .html, etc.) for each file.

For some reason, Windows considers this classified information!

To make the file extensions show up, click "Start" then "Control Panel." Double-click "Folder Options" then click the "View" tab. Scroll down the list and uncheck the box that says "Hide extensions for known file types."

You will now see the file extensions any time you open up Windows Explorer.

About the author:

Jim Edwards is a syndicated newspaper columnist and the co-author of an amazing new ebook that will teach you how to use free articles to quickly drive thousands of targeted visitors to your website or affiliate. Visit: www.TurnWordsIntoTraffic.com

How To Keep Your Computer Virus Free

by Otis F. Cooper

Computer viruses can and do strike at any moment. They assault your computer by destroying data, and rendering your system useless. The very first line of defense is to boost your knowledge of these well hidden malicious codes.

Malicious codes come in three basic formulas:

Viruses are small programs that reproduce themselves for the purpose of causing some damage.

Trojan Horses are disguised as gifts which may come as an attachment in your email. Once ran its purpose is to cause do harm to your system as well.

Then you may come in contact with **worms** which cause damage by copying themselves over networks as wells as individual systems. These codes alters not just one system but several within a network.

After you enhance your knowledge of malicious code, know the symptoms of an infected system. Strange PC behavior, an increase or decrease of data in a file, pop up messages, random graphics, and files being deleted are some symptoms of your system having a virus.

The best way to find and remove viruses is with the installation popular anti virus software from Norton or McAfee. These programs readily identify infections as well as promptly remove them.

Norton Anti virus installs easy and a configuration wizard runs after the computer has been re-booted. This software offers several options that give you the best virus scanning options. Use the neat update feature to keep up with all the new viruses. Their user friendly configuration leave no doubt in what and how you want this software to perform.

What should you do to prevent virus infection if you don't have anti virus software installed on your PC? We should all give a word of thanks for the Internet. Rush over to one the free virus scanning services which will scan your hard drive for malicious codes.

Trend Micro's Housecall scans your drive for viruses, trojans and worms. They ask you to register first but you can scan without registering. Why not go over to <http://housecall.trendmicro.com>

Visit Symantec's Security Check site and download their scan for viruses software which check your PC for possible infections of any malicious codes. Go to http://security.norton.com/ssc/vc_scan.asp

Don't do it.

Don't say, yes, I will get anti virus protection soon.

It will be when you wait one day too many and realize your computer must have a virus because it is deleting files, randomly showing graphics, performing one task when it should be performing another task, and other strange things. Take the time or invest the money for virus protection right now.

About the author:

Otis F. Cooper is solely dedicated to boosting the knowledge and confidence of every computer user that is serious about knowing computers. Use his informative articles and videos to understand every aspect about the PC.

Read more about his formula for pc training at:

<http://www.ultimatepcrepair.com>

and subscribe to the only newsletter with video clips showing you step by step PC repair procedures.

Internet Safety

by: Sharon Housley

Parents are constantly struggling with ways to keep their children safe online.

The Internet has a global reach and at this point no bounds, or limitations.

Outside of installing filtering software children should be educated in order to protect themselves to this virtual monster.

We've put together a collection of ten tips that should be observed while surfing online. At the very least these tips will prompt family discussions regarding safety.

1.) When on the Internet personal information should be kept private. Just because someone asks doesn't mean you need to tell them. When someone asks for personal information, consider how they might use that information and whether it is necessary for them to have it.

2.) If you are conversing with someone online, don't assume that they are being honest with you. Just because they say they're 16 doesn't mean they are.

3.) Do not release your password to anyone, even if they say they are from your online provider.

4.) Overall it is best not to respond to unsolicited e-mail (SPAM), if there is something flagrant or inappropriate in the e-mail, consider reporting the sender to their Internet Service Provider (ISP).

5.) Do not give out or post identifying information, including address or telephone numbers.

6.) You may want to create a nickname for a screen name in chat rooms.

7.) Keep in mind when posting in chat rooms or newsgroups, that there may be lurkers (people who read but do not post). Your information can be read and seen by all.

8.) Keep an open dialogue with children surfing the Internet, remember if they come to you with a problem, your first reaction should not be to take away the Internet. Applaud child's confidence in confiding in you and work together to find a solution.

9.) Overall it is not a good idea to post or exchange pictures over the Internet

10.) Try to keep in mind the Internet is global and is **not** governed by any entity. This means that there are no limitations or checks on the information posted and accessible to Internet users.

Additional Resources:

The following resources will assist in staying safe online.

Collection of Internet Access and Filtering Software

<http://www.monitoring-software.net/access-monitoring.htm>

Contract for Safe Surfing -

<http://www.911paging.com/internetsafety/internetcontract.htm>

About The Author:

Sharon Housley manages marketing for NotePage, Inc.

<http://www.notepage.net> a company specializing in alphanumeric paging, SMS and wireless messaging software solutions. Other sites by Sharon can be found at <http://www.softwaremarketingresource.com> Additional articles can be found at

<http://www.small-business-software.net/free-website-content.htm>

Beginner's Guide to Music File Formats

by: Gary Hendricks

Are you confused by the various types of music file formats out there?

Most of you would have heard of the popular MP3 format, but are you aware there are other alternative digital music formats like WAV, WMA, RA and MIDI?

Some of these give better sound quality than MP3 (e.g. the WAV format) but also need more disk storage space. Others like WMA give file sizes smaller than the MP3 format and are more suited for portable music players.

Let's run through the various file formats now:

The MP3 File Format:

MP3 files have the extension ".mp3" and are available for download from many web sites. MP3 (MPEG-1 Audio Layer-3) technology compresses a sound sequence into a very small file (usually one twelfth of the original file size).

The designers of MP3 compression algorithm managed to do this by eliminating sounds that the human ear cannot perceive. While MP3 technology is impressive, it has been abused by music pirates. One can very easily create MP3 files from commercial CDs and make them available for download. The RIAA and major music companies have been cracking down on the distribution and sharing of MP3 files in this manner.

The WMA File Format

WMA (Windows Media Audio) is Microsoft's proprietary music file format that it is marketing aggressively. WMA files are smaller in size than MP3 files, but still retain a decent level of sound quality. This format is getting very popular in websites for sampling music and also in portable music players. However, whether WMA will overtake the popularity of MP3 remains to be seen.

The WAV File Format

A wave file is characterized by the file extension ".wav". This music file format provides raw, uncompressed audio data. Originally invented by Microsoft, wave files are still used widely (examples include your start up and shut down sounds in Windows). Audio quality is excellent, but the file size is huge. A full pop song in wave format may take up to 30 MB of disk space or more.

The AIFF File Format

The AIFF (Audio Interchange File Format) is a popular music file format used in the Apple Macintosh operating system. In a way, they are the Macintosh equivalent of wave files. AIFF files have the file extension ".aif" when accessed via a PC. They contain raw audio data (which result in excellent sound quality) but take up a large amount of disk space.

The MIDI File Format

The MIDI (Musical Instrument Digital Interface) file format was originally created for recording and playing music on digital synthesizers. MIDI files are very small in size. The reason for this is that the MIDI file only contains information on how music is produced (e.g. note-ons and note-offs). The sound card which plays back the MIDI file takes this information and plays back music using an in-built soundcard wavetable.

The RA File Format

RA (RealAudio) files support streaming technology. Created by Progressive Networks, an RA file is highly optimized for live, streaming audio from websites. RA files are best played back on RealAudio players which are freely downloadable from Progressive Networks.

Conclusion:

Well, that wraps up our coverage of the most popular music file formats out there. You may be interested to know that there are many software applications which can convert music from one format to another (e.g. MP3 to WAV or WAV to AIFF). Do a search for these applications at www.download.com

About The Author

Written by Gary Hendricks - <http://digital-music-guide.com>

5 Ways to Speed Up Your PC

by Jim Edwards

No matter how fast your processor and regardless of how much ram you carry, there comes a time when you realize your computer just doesn't run as fast as it did when you bought it.

Windows loads slower, programs take longer to launch, and, in general, your computer drags like it just came off a 2-night drinking binge.

If this sounds like your situation, these 5 tips should help you get some extra speed from your PC.

~ Disk Cleanup Utility ~

You may not realize it, but just because you finish with a file doesn't mean your computer does.

In many cases, if your computer's hard drive were a garage, you would have unused junk files piled 20 feet high and spilling out into the street.

Everyone should use the Windows "Disk Cleanup Utility" to delete old, unused, and temporary files that clog your hard drive.

Click Start, point at All Programs (or Programs), Accessories, System Tools, and click Disk Cleanup. Analyze your hard drive for files you can eliminate and it may shock you to see how much hard drive space (and speed) you can free up with a few clicks.

~ "Defrag" ~

Imagine a properly maintained hard drive as room the size of Wal-Mart filled with filing cabinets.

Now imagine ripping open every drawer of every filing cabinet, slinging the contents onto the floor and trying to find one document -that's a fragmented hard drive.

Sometimes lack of speed simply results from your computer working too hard to find the files it needs. You can solve this problem by "defragging" your hard drive.

Click Start, point to All Programs (or Programs), Accessories, System Tools, and click Disk Defragmentor. Choose the disk you want to defragment and expect to let the program run for several hours.

~ **Uninstall Unused Software** ~

We all maintain software on our systems we rarely, if ever, use.

That software can steal system resources. Click Start, Control Panel, and "Add Remove Programs" to pull up a screen that allows you to remove old programs you don't use anymore.

Simply select and uninstall all programs you know for sure you don't need or want.

~ **Buy More RAM** ~

Increasing your RAM, a computer's memory, can dramatically increase speed when running certain operations or programs. RAM costs so little now that you should install the maximum amount of memory your system can handle.

~ **"Stop Them At Startup"** ~

This operation requires a bit more technical savvy than the other four, so proceed with caution.

Many programs load into the system tray in the lower right of your computer's desktop and consume system resources even if you never use them.

Click Start, Run, type in msconfig, and press Enter. Click the "Startup" tab to see a list of programs that automatically start with Windows.

Clear the check box next to programs you know you don't want to load at startup. But don't clear any checkbox unless you are 100% certain of a program's purpose. Once you finish, click OK and it will prompt you to restart Windows.

About the author:

Jim Edwards is a syndicated newspaper columnist and the co-author of an amazing new ebook that will teach you how to use free articles to quickly drive thousands of targeted visitors to your website or affiliate links...Need MORE TRAFFIC to your website or affiliate links? Visit: www.TurnWordIntoTraffic.com

The Seven Golden Rules Of Data Backups

by: Keith Edmunds

Backups of company data are carried out for two main reasons.

The first is to cater for those times when a document is inadvertently deleted or damaged and you wish to recover the original document.

The second is as part of a disaster recovery plan in case something catastrophic happens to your computers (e.g., victims of a fire or theft).

Backups cost time, money and effort to implement, and they are of no value right up until the time you need them. This means they tend to be given a low priority, but ultimately they may easily represent the difference between your business surviving and failing.

In this TipSheet, we look at the most common mistakes businesses make with backups.

1. Backup often

Re-entering data is tedious and frustrating. Backing up your company data once a week means that the most you should ever have to re-input is one week's worth. Backing up your company data once a day means the most you should ever have to re-input is one day's worth. Frequent backups lessen the impact of data loss.

2. Don't keep any volatile data on desktop PCs

In many organizations, documents are kept on the hard drive of desktop PCs. It is unlikely that this is backed up regularly, if at all. A PC can easily be replaced: last week's quotations may not be so easy to replace.

In particular, check that email is not stored on the local hard drive (this is very common in small to medium size businesses). All documents, spreadsheets, email, etc should be kept on a central server, which is in turn backed up regularly.

3. Automate the backup process

Backups are tedious to do. At 6:30pm, most people would prefer to set off home or join colleagues in the bar rather than stay in the office to find the correct tape and start a backup. Automating tedious tasks means they get done.

4. Monitor the backup process

While automating backups is a good idea, do check that they are running correctly. Make sure new files are being backed up; make sure the files of new users are being backed up. A quick check once a week could avert a much more serious problem later.

5. Keep backups offsite

If your business premises suffer a fire or flood, it is likely that backup media will be lost as well. Fireproof safes only protect media for a given time, typically one hour - if you use one, check the manufacturer's specification. If you always keep your backup tape in the server then when it is stolen the thief will probably throw the tape away. It's worth nothing to him, but it could represent bankruptcy to you.

6. Produce a "backup recovery" manual

A major disaster is not the time to try to remember how to recover data from your backup media. Have an idiot-proof, step-by-step procedure written - with a copy stored off-site - detailing how to reinstate your company data.

7. Test the recovery procedure periodically

Without warning, give the backup recovery manual to a member of staff and see how long it takes them to recover data. Many organizations never do this! No one involved with creating the manual or the backups themselves should be involved in the test.

The results of the test should be analyzed and the manual updated accordingly. A recovery test should be carried out at least twice a year. This proves both that the backups themselves are usable, and that your organization understands how to use them if necessary.

About The Author:

Keith Edmunds has been helping companies get the most from their IT investment for over twenty years. He is the Managing Director of Tiger Computing Ltd <http://www.tiger-computing.co.uk>

Thinking of buying a laptop computer?

Then find out everything you need to know *before* you buy at:

www.HowToBuyALaptop.com