

Basics of System Maintenance, Security, and Data Synchronization

This document provides a high level and understandable view of how to maintain and secure your system and synchronize data such as files, contacts, bookmarks etc. across different systems and devices.

1. Introduction

The average new PC has more than enough resources to do anything you can imagine without the need for constant upgrades or buying new hardware and software, and most of the tools you need are free to use.

A well configured new PC can easily last 7 to 10 years and a new laptop 5 to 7 years with only a few essential upgrades, typically memory and additional storage space, but they rarely do. Why?

The answer is simple.

Besides all the well advertised viruses, malware, adware, etc. every piece of software or hardware you add to your computer increases the overall complexity of your system potentially pushing it ever closer to a breaking point.

Quite often the tools you buy or download to help maintain your system are the very things causing your system to become bogged down.

How can you know what is and isn't worth using?

2. The Deadly Twin Perils of Sprawl and Bloat

To begin:

Most proprietary systems (Dell, IBM, Toshiba, Acer, HP, etc.) come loaded with special partitions and applications to recover and maintain your system but most people don't know that they are there or how to use them. Unfortunately, many require a level of technical comfort with lower level hardware and computer operation that most people don't have such as accessing or modifying the BIOS and creating and using bootdisks from images. Worse, learning how to use one set of tools is often no help in understanding how to use the next set of tools that come with the next system.

Graphical User Interface based operating systems such as Windows were never meant to be this hard to use!

Many similar utilities also come as part of Windows itself, or are available for free, and software vendors and retailers are always extolling the virtues of this or that program as a way to secure and improve the performance of your system.

The amount of duplication and competition between these applications for system resources can gradually, or quickly, cause your system to fill up with unneeded data, Windows services, Startup programs, updater programs, registry entries, temporary files, uninstall points, system recovery points, and automatic updates that steal the very computing power you paid for.

What Internet browser on your computer is winning the default browser war, and how much performance is this battle costing you?

Worse still, many of these applications, widgets, plug-ins, add-ons, etc. themselves introduce vulnerabilities into your system requiring more time and expertise to address than most have the energy and knowledge to deal with.

Add to this the fact that most software does not completely uninstall, leaving behind miscellaneous files and permanently altering system configuration and you have still more accidents waiting to happen.

Should you be overly worried?

Not really.

For most of us learning some basic good practices and having a simple security and recoverability plan is more than enough. Like the bicycle owner that understands that a good lock makes a thief search out easier targets a savvy technology user understands that it doesn't take much to make a system a harder nut to crack than most of the other systems on the Internet.

It takes only a little help and a little bit of planning and knowledge to keep your system and data safe in the ever growing ocean of unsecured systems and data.

Virtual life is just like real life: basic knowledge and understanding is power and peace of mind.

We've picked on the technology providers enough. The other side of the coin is you.

What responsibility do you have for securing your own system and what are the consequences for you and others if you don't?

Experience has shown that the average person tends to create and store data indiscriminately in default locations mostly decided by the software and operating system with the result being **data sprawl** and **data bloat**.

Data Sprawl is the inadvertent and unintentional duplication or re-creation of data and applications that results from not knowing where your data is stored or by not understanding how to make that data accessible from multiple locations (file sharing).

Data Bloat is the tendency of system hard drives to rapidly fill up with software and data that is unneeded.

When sprawl and bloat combine valuable data and systems become less available to the person who created and uses them and, ironically, more available to those with malicious intent!

Add in all the software and operating system tools creating unneeded data or introducing vulnerabilities and you can watch the space on your C drive disappear daily. Windows Vista can grow in size by gigabytes every day.

Do most people understand and use any of the real power of Windows to prevent sprawl or bloat?

Not really.

Most of us simply accumulate data, applications, and devices willy-nilly until something breaks and then we are at a loss as to what to do. Often we lose all or most of our data, music, movies, documents, bookmarks, contacts, email, photos, and then start all over again with a new PC, new cell phones or new mp3 players doomed to the same end, all because we don't understand how our computers and technology are configured to work, or how they can be configured to work in the ideal.

If technology companies really wanted to help us they would teach us what we need to know, but they don't, and user manuals, help files, tech support, and on-line help are, for most people, ineffective.

How many times have you had to waste time and energy trying to get your software to stop 'helping' you or deciding what you are trying to do?

What if you could understand how to start with a system that does only what you want it to do and nothing more?

Here's how.

The simplest maxim that leads to a sustainable and secure system is this:

If it ain't broke don't fix it, but fix it first.

After you buy a new computer and start adding things left and right to get your basic system running you can rest assured that unless you understand and control all the changes made to your system that it is already broken and it's just a matter of time until something goes wrong that you have no idea how to fix or prevent from happening again.

Here are just a few things that can be done to control bloat and sprawl and to protect your system:

- Don't buy proprietary hardware unless you can start with a fresh un-customized version of the operating system without all the fancy partitions and system backup and restore utilities that no one uses
- Turn off System Restore and Indexing in Windows and instead use a simple manual backup and recovery plan or an automated one if you have more than one computer or prefer things automated
- Make sure your system has enough memory (1 GB for XP, 4 GB for Vista, more for Windows 7)
- Don't let your hard drive get over 75% capacity before off-loading data or upgrading storage
- Learn how to regularly disk scan and defrag your hard drive using built-in tools
- Install a second internal or portable hard drive for simple manual backups
- Configure Windows update and software updates to run less frequently and late at night

- Remove unneeded system software, updating programs, toolbars etc. that bog down your system
- Do research from at least three different sources before adding any hardware or software to your system: on-line, trusted retail technology businesses, and friends or family you consider technology savvy
- Don't believe the hype – it's mostly hype!
- Learn how to better install and configure your software by doing custom installs and configuration before you start using it
- Learn how to create your own folder structure and manage your data and stop relying on default software and operating system configurations
- Stay away from most if not all software that is supposed to improve system performance, clean your registry, update your drivers etc. At best this stuff does nothing, at worst you are downloading malware

3. A Basic Maintenance Strategy

Problems are inevitable even for an optimally configured system.

How can you minimize the impact and down-time?

If and when a critical system problem arises due to software or hardware issues, or viruses and/or malware it often takes more time and money to fix than to simply restore your entire system. To do this efficiently you need a data and system recovery plan. This involves a simple software tool, some form of external data storage, and learning enough about your technology to be able to use it wisely.

Even if you have no money in the budget for software and hardware you can leverage all the free software and services on the Internet to do this inexpensively and simply, but you'll need someone to help you get started.

Your existing or new system can be reinstalled and/or re-configured for the best possible long term performance and security, and you can be shown how to maintain it at a level you understand.

The key part of the strategy is to take and store an image (a single digital copy of the contents of your hard drive) of your system that can be quickly and inexpensively recovered and brought up to date.

Once the system is restored and updated from its last stable configuration simply restore all your backed up data (including things like contacts and bookmarks), take a new image, and you're back up and running in no time.

No licence keys, no starting from scratch, no lost software or data!

If you're not a big tinkerer you may only need to restore your system once or twice for the 7 to 10 years the system is actually fast enough to do what you need and want it to do. If you like to tinker a lot or run resource intensive applications such as video or digital editing or on-line games a

simple imaging strategy and back up system frees you to break and fix your system effortlessly, as often as you wish, while maintaining a fast and clean running system.

We can even teach you to do this for yourself and you can take us right out of the equation.

4. The Basic of Security

The reality of security on the Internet is simple; the only sense of security is a false one.

The way the Internet was envisioned and implemented was for it to be as fault tolerant as possible, and it is. The sheer mass of data that is transparently and reliably sent zooming around the world and into near-space is unfathomable! We take for granted that the technological miracles, which allow you to effortlessly and instantly send a photo you just took at your son's wedding to your brother teaching High School in Korea from your Blackberry, simply work, or if they fail will let you know!

If security was the primary goal in how the Internet was designed and implemented these things would be much, much harder and more expensive to accomplish, and much less reliable!

Security was added on later as the initial military project that led to the creation of the World Wide Web involved using wires that were meant to stay hidden and not accessible to the general public.

Many different technologies are in place to secure Internet traffic at its most basic level but are not generally in use. Most Internet data and system security is implemented at higher levels such as in applications and only works if properly implemented and maintained, and if everyone agrees to behave!

The end result is that almost every system on the Internet can be directly or indirectly compromised, even at its most basic level.

All it takes is someone with the basic technical skills and the motivation to do so. Most security systems only work because people agree to use them the way they are implemented, but why would an attacker try to break down a heavily fortified door when a window is open.

The only way to be secure in terms of things you can control is by learning and adapting the right behaviours, not by relying on software, hardware, other people, or institutions to keep you safe.

It's your data and information after all.

I, personally, have had a Gmail account for 8 years and only recently started getting spam because I fell for a very well constructed social engineering ploy that appealed to my vanity, and exploited a well known website. Boy, did I feel silly.

I have on occasion had real nasty malware that has compromised my systems but I typically have computers that are 4 -5 years older than anyone else's, run trouble-free for years, and often get them for free because people think they are too slow or old.

Nothing could be farther from the truth as I type this on a 4 year old Acer laptop that was originally doomed to disposal!

Did you know that:

- ***a simple Linux bootdisk is all that's required to reset Windows XP passwords?***
- ***many service providers send you email with your password in plain text and that most email can be easily intercepted and read?***
- ***any password less than 8 characters is almost useless if someone really values access?***
- ***as many as 30% of the PCs on the Internet are compromised by malware***
- ***governments are even designing their own malware!***

What can anyone possibly do to deal with this mess?

The simplest thing is to simply disconnect your computer from the Internet when you aren't using your computer, but that doesn't make much sense, does it?

But, how do you choose what tools and behaviours to use?

The problem is simple: sometimes the free programs are all you need, sometimes it's better to pay money but the reality is that every 6 months to a year everything changes.

For example, really good freeware often gets bought out and the new owner then fixes it to the point that it starts to bog down your system or becomes less effective than other products. This recently happened with AVG Free.

Currently installing 2 or 3 different free tools covering viruses and malware primarily is recommended. Configure one to run daily or weekly and automatically update. Run the others manually on occasion or if you suspect a problem.

Or: buy a single simple retail product that does it all.

Do your homework before installing or purchasing. Don't install and then uninstall if you aren't happy with the program as this can lead directly to the same sorts of problems that the viruses or malware cause!

Spybot, Adaware, Windows Defender, A2Squared, and Avast are decent current free choices, but this will change with the weather!

Kaspersky products are currently a better retail choice and their products can do the same as a bunch of free ones and don't bog down your system too much.

Large corporate products such as Norton, Spy Doctor, and McAfee are often way too complicated, interfere way too much with the smooth running of your system, and don't uninstall properly.

The more aggressively the products are marketed and the slicker the marketing the more suspicious you need to be. Don't trust the results of any free downloadable or on-line scans or trials!

Finally, if you don't have a properly configured and maintained hardware firewall/NAT router in place you might as well unlock all the doors in your home, car, and office too. The result is the same!

In the end it is best take ownership for your data and systems and the choices you make when you use your technology. If you allow your computer and data to become compromised out of ignorance or neglect then not only are you responsible for any losses you experience you are also responsible for what the malicious hackers do with your data and system such as seeding malware, sending out spam, hosting denial of service attacks, etc.

The best way to make the Internet safe and reliable is for individuals to take the basic steps necessary to learn how to secure and maintain their system themselves!

If you leave a loaded gun on the coffee table with the safety off whose fault is it when something bad happens?

Here are just some critical behaviours to learn and adapt to make your system and data safe even if you have no extra software protecting you.

- Research, research, research from different sources before you buy or try
- Don't download indiscriminately or impulsively. **This will guarantee your system becomes infected and data lost.** Any time you feel the impulse to click this or that flashing icon or download this or that cool application **BEWARE!**
- Avoid using any peer-to-peer applications unless you really know what you are doing. Pay for some basic system configuration and training and do some research before starting.
- Use sandbox or virtual OS tools to test out new software before installing it on critical systems
- If it ain't broke don't fix it, but fix it first!
- Use a simple password management system with three levels of passwords. Use secure passwords and don't share them. Don't use the same password for every site! Keep your bank card password and/or online banking password completely different from other on-line passwords
- Assume that everything on your computer could be made public to the whole world and protect sensitive information accordingly. If you don't want others to access any of your data then either store it off-line or encrypt it!
- Create a second and/or third free email account to use for joining on-line services that is separate from your most important email address; the one you use for important personal and/or business email.
- Stop expecting other people to protect you and take steps to learn how to protect yourself
- Accept that risks are only minimizable and can't ever be reduced to zero!
- Have a simple backup and recovery plan in place

- Be careful about what information or data you post on-line, especially on social-networking sites
- Don't forward or open attachments from any source unless it is data you know is safe and that you have requested
- Don't send or receive large numbers of files, or files larger than a few MBs in email. Set up a personal FTP server, or use free web space and put download links in your email
- Don't share USB keys or portable hard drives. Many sorts of malware are transmitted directly this way
- Manually update and scan your PC at least once a month even if the software is configured to do this automatically. The same is true for patching software and your operating system updates

5. Basic of Data Synchronization

mp3's, documents, avi's, jpgs, images, movies, ebooks, software, bookmarks, contacts, passwords, email, photos, favourites, tags, lists, add-ons, toolbars, etc.

These sorts of data define how and what you use the digital world for.

Do you know where all this data is stored?

Do you know if it is secure?

Can you access it when and where you want to?

Do you have an organized and centralized database or main application for all the contact information store on your cell phone, in Skype, in Outlook or Gmail, in iTunes, or is this information spread out in multiple 'silos' (remember sprawl)?

If you are like most people your data is spread out over many applications, not particularly well-organized, stored in places that Windows or your applications decided and that you may or may not be aware of, not backed up, and not very secure.

For some this is not a concern, but with every passing year our information and the things we create with our technology is becoming more important in both our personal and professional lives.

Information IS power. Information IS Possibility.

Do you treat your information as if it is valuable or expendable?

Would you like to have better control over your technology and all the stuff you create with it?

Would you like to know that it is organized, secure, backed up, and available anywhere?

Here are some basic pointers to help you organize your data:

- For every application with contacts or bookmarks find out where the user information is stored and manually back up user files, the whole profile, or export contacts or bookmarks to a simple spreadsheet such as Excel or Calc (The spreadsheet format is generally very portable between many applications).
- Explore all your software that has stored information you value to discover how you can back up, import or export this data
- Most cell phones come with applications to import or export contact information and/or files. New devices can be preloaded with contact information from any other source
- Record basic hardware and software configuration about your computer such as passwords, amount of memory and hard drive space, what video, LAN, sound card, etc. you have in your PC, what type of memory, your Windows license key, any information that helps when the time to upgrade, problem solve, or rebuild Windows comes (when it comes its often too late to simply recover this information)
- Learn how the basic folder structure in Windows is set up and works so that you can create your own folder structure and file naming conventions and stop relying on defaults.
- Create 3 deliberate copies of valuable files or data, with at least one copy stored off-site. This 3 copy, 2-site model of backing up is the minimum for covering all likely and unlikely events that might cause the loss of data
- Learn how to remotely access any or all of your data wherever you have an Internet connection to and from your home or office
- Use free or paid services to store data on-line, backup bookmarks, etc. Many excellent services are available

It is possible to set up and maintain a simple system for taking control of your data and technology no matter your level of experience or comfort with technology. Simply identify what is valuable to you and imagine, in the ideal without worrying about any details, how this system would work.

**Let us help you make a fresh start
and create a data and technology world that works for you.**