

Copyright and Disclaimer

The ebook is protected by US and International copyright law, and is Copyright © 2008 by Leo A. Notenboom and Puget Sound Software, LLC, all rights are reserved.

Having said that, this ebook is FREE. If you wish, you are free to share this ebook with others as long as you share it:

- In its entirety (the whole book and only the whole book)
- In its original form (no changes are made and no markups are added)

You may not charge for this ebook when you share it. Furthermore, you may not incorporate this ebook into any product or collection that is not free.

This book is based on my experience and anecdotal evidence. I've tried to ensure that everything written here is as accurate as possible at the time of publication, but I cannot assume any responsibility for mistakes or omissions.

On top of that, I know nothing about your specific computer, your specific experience and your specific abilities to understand and act appropriately on the information herein.

The bottom line is that you, *and only you*, are responsible for using this information appropriately, safely and as you see fit, and for any of the consequences of having done so.

Note that any trademarks, service marks, or product names are the property of their respective owners. There is no implied endorsement when I reference something by name. Endorsements, if any, will be clear and quite explicit.

Finally, this book is intended to inform and entertain, but it's still not a replacement for common sense. ☺

Contents

1. Virii & Spyware & Worms ... oh my!	4
2. Use a Firewall.....	6
What's a firewall, and how do I set one up?.....	7
Do I need a firewall, and if so, what kind?.....	9
Do I need SP2's Windows firewall or not?	11
3. Scan for Viruses	12
Viruses: How do I keep myself safe from viruses?	13
I run anti-virus software, why do I still sometimes get infected?	16
When do I actually need to run a virus scan?.....	18
4. Kill Spyware.....	19
How do I remove and avoid spyware?.....	20
So just how sneaky can spyware be?.....	22
5. Stay Up-To-Date.....	23
How do I make sure that Windows is up-to-date?.....	24
6. Get Educated	26
Phishing? What's Phishing?.....	27
How do I get rid of all this spam?!?!	29
7. Secure Your Mobile Connection.....	31
How do I stay safe in an internet cafe?	32
Can hackers see data going to and from my computer?	34
8. Don't forget the physical.....	35
How can I keep data on my laptop secure?.....	36
What backup program should I use?.....	38
That's It, And Yet.....	40



1. Virii & Spyware & Worms ... oh my!



© [Piksel](#) | Dreamstime.com

These days the very concept of "Internet Safety" seems like an oxymoron.

Not a day goes by where we don't hear about some new kind of threat aimed at wreaking havoc across machines connected to the internet. While products other than Microsoft's are certainly vulnerable, anti-Microsoft sentiment coupled with the massive installed base make Microsoft products an irresistible target for hackers and "script kiddies".

In this book we're going to cover the basics - the things you must do, the software you must run and the concepts you need to be aware of - to keep your computer and your data safe as you use the internet.

It's not hard, and once things are in place it's not even time consuming. But it is necessary.

Let's summarize what we're going to cover:

- **Firewalls** - the first line of defense protecting your computers from threats. Without a firewall your computer can be compromised within seconds of simply being connected to the internet.
- **Viruses** - the threat is real and changing every day. Machines get infected quickly and easily if you don't take steps to protect yourself.
- **Spyware** - from popping up annoying ads to capturing your sensitive data, spyware, much like viruses, continues to be an on-going and growing threat.
- **Staying Up To Date** - one of the most surprising statistics you'll hear are how many machines are not protected simply by not being up to date on patches. Many, if not most, malware infections never need happen.
- **Education** - Are you the weakest link? All the protective software and hardware in the world can't protect you from yourself.
- **Mobile** - Portability, Wireless technology and Wi-Fi hotspots open up an entirely new venue for security and privacy related issues.
- **Physical** - Perhaps *the* most overlooked aspect of all, a hacker could "own" your computer in moments in very common and simple circumstances.

This ebook is based on articles originally published on [Ask Leo!](#) which represent real questions and real problems faced by real people just like you.

I've collected these articles together to give you an overview of the basics of what it takes to keep your computer safe.

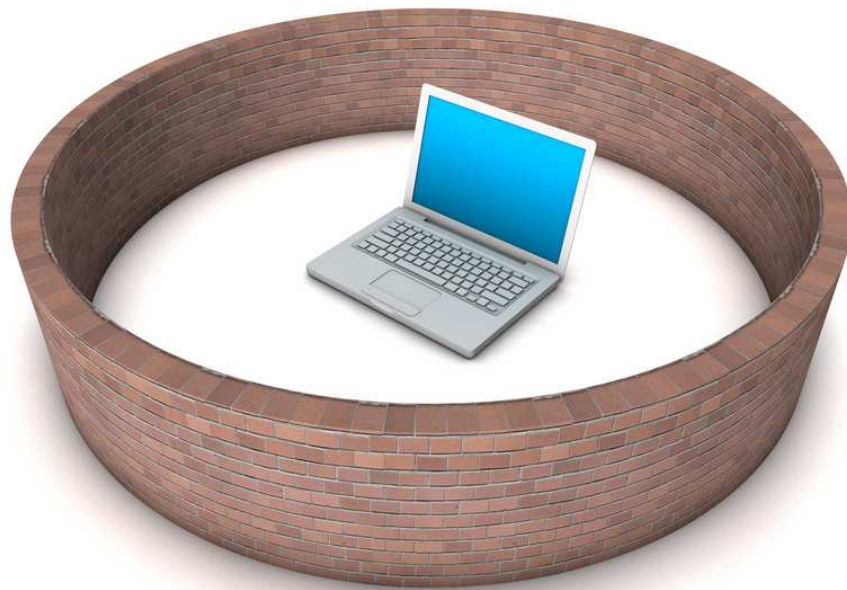
And I'm giving it away because it's just that important.

And of course I hope that you'll be interested enough in learning more to come visit [Ask Leo!](#) to read more about these topics and much, much more, or to ask questions of your own.

Let's begin.



2. Use a Firewall



© [Matthiashaas](#) | Dreamstime.com

A firewall is a piece of software or hardware that sits between your computer and the internet and only allows certain types of things to cross the wall. For example, a firewall may allow checking email and browsing the web, but disallow things that are commonly not as useful such as RPC or "Remote Procedure Calls". In fact, it's vulnerabilities in RPC that allowed for one of the more recent worms to propagate.

What's a firewall, and how do I set one up?

Viruses like the Sasser worm can be prevented simply by using a good firewall. What's a firewall? Well, in your car it's the "wall" of metal behind the dashboard between you and the engine that prevents engine fires from roasting you and your passengers.

A firewall for your computer is much the same - it's to keep you from getting burned.

A firewall's purpose is very simple: to block or filter certain types of network traffic from reaching your computer. What do I mean by "certain types"? There are things you want to get like the pages of web sites you visit or the software you might download. And then there are other things you might not want like people accessing your computer remotely or viruses and worms infecting your machine.

A firewall knows the difference.

Firewalls are also usually configurable; they can allow you to say "this kind of connection from the outside is OK". A good example is Remote Desktop. A firewall will by default prevent it from working. But you can also configure the firewall to allow that type of connection to come through. That way you would be able to access your computer from another, across the room, or across the internet. But other types of traffic like viruses are still blocked.

Some firewalls will also monitor outgoing traffic for suspicious behavior. One characteristic of many viruses is that once you're infected they attempt to establish connections to other computers to spread. Many software firewalls will detect and either warn you or simply prevent it.

And that leads to a very important distinction in firewalls - there are two types: hardware and software.

- A **hardware** firewall is just that - a box that sits between you and the internet that performs the filtering function. Traffic that is filtered out never reaches your computer. Broadband routers perform the function of a firewall quite nicely and are typically what I recommend. The downside for hardware devices is that most will not filter outgoing traffic.
- A **software** firewall is a program that runs on your computer, and at the very lowest level monitors your



If you're using a phone to dial-in to the internet, a firewall is not quite as important, though it doesn't hurt to have one. A software firewall may be your only option, though.



network traffic. The firewall prevents filtered traffic from getting through to the operating system. All network traffic reaches your computer but the firewall prevents your system from actually doing anything with it.

The good news is that if you're running Windows XP, you already have a firewall built-in. It's a simple matter of turning it on to get the protection you're looking for.



Do I need a firewall, and if so, what kind?

The very short, very easy answer is: *hell yes!* With all that's happening on the internet these days it's simply too risky to sit "naked" on the internet unless you really know what you're doing.

The real question is: what do you need? It's even possible you already are behind a firewall and don't need anything additional.

First, realize that a firewall is about protecting you from them, where "them" means "the malicious folk on the internet". A correctly configured firewall does not block your access out to the internet so you should be able to browse the web, for example, without interruption. The firewall prevents access from somewhere on the internet to you. That's not to say people can't send you email; they can because you access your mail through the internet when *you* retrieve or download it. It does mean that people can't copy files directly to your PC or cause programs to be run on your machine.

Step one is to check with your ISP. Some actually do provide a certain amount of firewalling. AOL, if I'm not mistaken, is a fairly good example: they've set up their own private network and internet access is tightly controlled. The good news is that you may be well-protected. The bad news is that you have no control over it, and you may not be protected from other AOL users. Most ISPs, however, do not provide any kind of firewall. What you get from them is a direct connection to the internet. That gives you the most flexibility and control but it also places the burden of protection in your lap.

The next question is do you need a hardware or software-based firewall? In my opinion, if you connect via broadband such as cable or DSL then there's no question at all: broadband routers are inexpensive and provide an exceptionally high level of protection out of the box. They're typically easy to set up and also have the flexibility to be carefully configured for more advanced uses such as running a web server from behind your firewall. I like the hardware approach because the routers are devices dedicated to their task and do not interfere with - nor can they be compromised by - your computer. Remember, a router will work fine even if you have only one computer.

[Ask Leo!](#) - You can read more about how I'd set up a home network using a router in the article [How should I set up my home network?](#)

If you are on dialup or have some other reason for not wanting to go the hardware route there are software firewalls as well. In fact, Windows XP includes one by default: on the properties page of any network



connection, click the advanced tab and you'll find the **Windows Firewall**. Even if you do nothing else and you're not sure what you really want to do, you should turn this on. Other popular firewalls include [ZoneAlarm](#) and [Comodo](#).

Finally, when you believe you're protected or even if you know you're not you should visit [Gibson Research](#) and run "Shields Up", a vulnerability analysis. It will try to access and analyze your computer from the internet, list for you exactly how you are vulnerable, and tell you the potential steps you can take. It tends to be a little techie but it's worth the effort.



Do I need SP2's Windows firewall or not?

There's a lot of misunderstanding about firewalls, routers, and other security software. Windows XP2 SP2 definitely puts security and particularly the firewall, "in your face", so it's a great opportunity to find out what you need and what you don't.

As discussed earlier, a firewall filters incoming traffic. The bottom line is that a firewall protects you from certain classes of incoming problems.

Everyone should have a firewall of some sort.

In general hardware firewalls, typically provided by NAT routers, keep malicious traffic from ever reaching your computer, whereas software firewalls, such as the Windows firewall, discard malicious traffic after it has actually arrived at your computer.

But you don't need both.

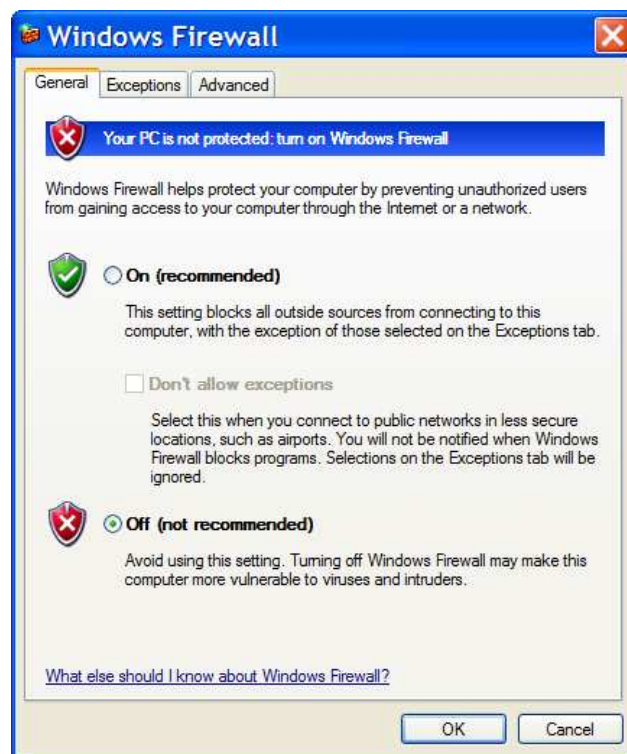
If you have a router with NAT enabled, then there's no need to enable the Windows firewall. In fact, you can tell the new Windows Security Center that you'll manage your firewall yourself

If you're not behind a router or other firewall, you'll want to turn on the Windows firewall. This is what I do when I take my laptop with me on the road.

Now, one word that arises when discussing the difference between firewalls: "outbound".

Firewalls typically handle protecting you from incoming traffic. Neither a typical router, nor the Windows firewall, will filter or manage outgoing traffic. For that you need either a significantly more expensive industrial strength router, or one of the more complete firewall and security packages such as ZoneAlarm.

Personally, I'm quite happy behind a router, and if you're behind one, I don't commonly see a real need for the added expense.



3. Scan for Viruses



© [Devonyu](http://www.Devonyu.com) | Dreamstime.com

Sometimes, typically via email, viruses (or virii) are able to cross the wall and end up on your computer anyway. A virus scanner will locate and remove them from your hard disk. A *real time* virus scanner will notice them as they arrive, even before they hit the disk, but at the cost of slowing down your machine a little.

Important: because new virii are arriving every day, it's important to keep your virus definitions up-to-date. Be sure to enable the scanning software's automatic-update feature and have it do so *every day*.

Viruses: How do I keep myself safe from viruses?

Computer viruses are a fact of modern, internet-connected life. At best, they're annoying performance sucking beasts, but at worst ... kiss all your data good bye.

We **all** need to take steps to make sure that our computers are safe, or we risk infection. Complacency is not an option.

And yet, even after all the news, and all the warnings, and after all this time...complacency remains all too common.

There are four important steps:

1. Install and Run an Anti-Virus Program

There are many out there.

Personally, I run Computer Associate's [eTrust AntiVirus](#). It was the corporate standard solution [where I used to work](#), and has served me exceedingly well for several years now. I have it scheduled to update signatures and scan every night.

I've also heard good things about [Panda Antivirus](#), [AVG Anti Virus](#), and [Kaspersky Anti-Virus](#). Symantec maintains one of the best [reference sites](#) for virus related security issues.

Free and On-Line Virus Scanners: I've learned that not all virus scanners catch all viruses. I recommend having a selection of free virus scanners to run as a "second tier". [AVG](#) has a free product. [Trend Micro's Housecall](#), and [Panda's Active Scan](#) are on-line scanners that download as an ActiveX control in your browser. Most downloadable virus scanning solutions often include free trial periods that can also come in handy as one-time second-level scans.

2. Update the Anti-Virus Database

Your first step should be to update the virus signature database that came with the installation. New viruses are being created every day, and the databases that the anti-virus programs use are being updated as well. You need to get the latest database for your program right away.

Most of the programs have update functions that will locate, download and install the latest databases automatically. Make sure that this is enabled.



3. Run Regular Scans

Most of the anti-virus programs work automatically. Once installed they are configured to scan all incoming and outgoing files, and often hook into your email, in some way, to double check that your received email is clean as well.

Unless you know what you're doing, make sure that this "real time" scanning is enabled.

I also recommend periodically running scans of your hard disk(s). Certainly when you first install the software you should run a full scan. Then, depending on how heavily used your machine is, you should run a scan periodically as well.

Some programs will allow you to schedule such a scan to happen automatically. In my case, for example, since my computers are on 24 hours a day, I schedule full virus scans nightly, while I'm asleep.

4. Keep Windows Up-To-Date

We'll talk more about this later, but visiting [Windows Update](#) regularly, or simply enabling the automatic update feature in Windows is an important part of avoiding many viruses.

All software has bugs. Some of those bugs are used to create the exploits that virus writers take advantage of to create viruses that can infect your system. As these bugs are found, Microsoft fixes the affected components in the operating system, and makes those fixes available for download and install using Windows Update.

The "problem", is that even once the bugs are discovered and publicized, and even when the fix is available, virus writers get busy writing viruses that still exploit them. Why? Because **they know not everyone stays up-to-date.**

Keep Windows up-to-date. Let someone else have the "fun" of being infected with the latest viruses. Visit [Windows Update](#) weekly, or enable automatic update.

Ask Leo! - One of the *most popular* articles on Ask Leo! is being read by thousands of people each month who are still being affected by a virus using an exploit that was patched *over two years ago*:

[What are "LSASS", "LSASS.EXE" and "Sasser" and how do I know if I'm infected? What do I do if I am?](#)

Additional Notes

Sadly, there is no "best" anti-virus program. Each may miss some something that the other's catch. That's one of the reasons I list several.



The best advice is to use one, any one, and have the others "on call" for those cases when malware sneaks past the one you use regularly.

If you do install more than one package, you should **not** enable the "real time" scanning for more than one at the same time - they will conflict with each other, and will cause unpredictable results.



I run anti-virus software, why do I still sometimes get infected?

It's a good question. And the answer is partly the nature of anti-virus software... and partly the nature of "the race".

The Race - And Bad Luck.

I use that term on purpose. Combating viruses is a race between virus writers looking for vulnerabilities, the team of anti-virus software vendors looking to catch them, and system software providers looking to plug the security holes that viruses exploit.

So the first answer boils down to bad luck. It's possible to be doing everything right, and still get infected if you catch a new virus before your anti-virus software knows how to detect it and before your system software has been patched to disable it.

All Anti-Virus Software is the Same, Only Different.

Sadly, as far as I can tell, there's no "best" anti-virus package. Most all of the name brands are good, but I've not run into one that really stands out above the crowd as detecting absolutely everything.

What that means to you is that no matter what anti-virus package you run, it may miss something. Different packages may miss different things, but there doesn't seem to be a single package you can count on to catch everything. So it's possible to still get infected even though you're up-to-date with your package.

The Internet - Wear Protection Before Touching It

One of the more frustrating scenarios in recent months involves going through great lengths to clear a machine of viruses, only to get infected again within seconds of connecting to the internet. Some viruses exploit operating system vulnerabilities that are present simply by connecting to the internet. You don't even have time to download your operating system update, or anti-virus software, before your machine is once again a victim.

As we've already discussed, firewalls help. That's one of the reasons folks like me harp on putting your computer behind some sort of a firewall. Firewalls understand the difference between certain types of legitimate internet traffic, and types that you'd never need. They block out the unwanted stuff before your computer ever really sees it, or has a chance to be infected by it.



A Virus is a Trojan is a Worm is a Virus

All viruses are not created equal - hence all the different terms used to describe them. Some exist merely to propagate, others exist to do damage, while still others start to blur the line between virus and spyware as they install monitoring or additional vulnerabilities on your system. Some travel by email, others by downloaded applications, and as we just saw, others can travel from unprotected computer to unprotected computer directly through the internet.

Ask Leo! - All the different terms don't help clear the confusion either. If you're curious, check out this article on Ask Leo!: [What's the difference between a 'Trojan Horse' a 'Worm' and a 'Virus'?](#)

Anti-Virus programs have a hard time protecting you from yourself. For example, if you open an email attachment you don't recognize and run it, you may install a virus before your anti-virus software has a chance to act. If, when downloading a file, you choose to ignore a warning that your anti-virus package or firewall throws up, you're telling the software that you know better than it does what is or is not safe. Let's hope you do.

Why?

Why is it like this? It's hard to say. Ask 10 people and you'll get 10 different answers. Hackers with too much free time. Operating systems that aren't robust enough. Success in the marketplace makes for a bigger target. And more.

What we do know is that it is like this, and will be for the foreseeable future. That's why, ultimately, you and I are responsible for keeping our computers safe on the internet.

When do I actually need to run a virus scan?

Virus scanners are best used to *prevent* viruses from ever reaching your machine, but this raises an issue that most folks don't realize.

There are two types of scans.

One type of scan is the continuous "real time" scan that watches for viruses in data as it arrives (or possibly as it leaves) your computer. Typically the scanner will hook into your network connection and simply watch the data coming and going to and from your machine, watching for viruses. If it sees one then it takes action and alerts you. These are definitely the safest. For example, a virus in a download will be caught before it's ever had a chance to run on your machine. Some will also prevent email-borne viruses from arriving in your inbox as well.

It's important that there be only one real time scanner running at a time, as they can conflict with each other. But one is all you need.

The other type of virus scan is an "on demand", or scheduled scan. This is when you ask your virus program to scan the contents of your hard disk for viruses. It then scans your machine, reading every file for possible viruses. Naturally reading everything on your hard drive can take a little while.

The free virus scans are typically this type. You initiate a scan, and a while later the scanner tells you whether or not your machine was infected and whether or not it was able to remove the infections.

Most anti-virus programs include both types of scans; real-time and on-demand. I advise having a couple of additional on-demand scanners ready (or at least selected) when it comes time to track down a particularly nasty virus that perhaps your regular virus scanner misses.

For what it's worth, I normally don't run a real time scan since I'm fairly well protected in other ways. I do, however, run an on-demand scan which is scheduled every night.

Critical to all this, of course, is that you make sure that the database of virus definitions your scanner uses is as up-to-date as possible. I make sure to downloading the latest database for my anti-virus software every night.

Whether you run a real-time scanner or a nightly or periodic scan, remember that it's critical to do *something*. The days of being blissfully ignorant about viruses is long past. Without virus protection you are setting yourself up for some serious problems down the road.



4. Kill Spyware



© Bobb | Dreamstime.com

Spyware is similar to virii in that they arrive unexpected and unannounced and proceed to do something undesired. Normally spyware is relatively benign from a safety perspective, but it can violate your privacy by tracking the web sites you visit, or add "features" to your system that you didn't ask for. The worst offenders are spyware that hijack normal functions for themselves. For example, some like to redirect your web searches to other sites to try and sell you something. Of course some spyware is so poorly written that it might as well *be* a virus, given how unstable it can make your system. The good news is that, like virus scanners, there are spyware scanners that will locate and remove the offending software



How do I remove and avoid spyware?

It's a modern scourge. It's certainly on the top 5 list of topics I deal with on a regular basis. Some actually live up to the name - "spy" ware that actually monitors what you do. Others are worse: acting almost like viruses, hijacking your web browser, popping up ads, or just generally wreaking havoc. Unfortunately the reality is that it requires vigilance on everyone's part to control it.

Besides taking normal precautions, you *must* scan for spyware.

There are three important steps:

1. Install and Run an Anti-Spyware Program

There are many out there, but popular recommendations usually boil down to:

- [Windows Defender](#) - Microsoft's entry has received good reviews and some are reporting that it's catching more spyware than other entries in the anti-spyware arena. It's free.
- [Spybot Search and Destroy](#) - Spybot is free and does a great job of ferreting out and removing spyware. Spybot is one of the most commonly recommended tools when people are dealing with spyware issues. It also includes options that will help "immunize" or prevent certain types of spyware issues from occurring in the first place.
- [Lavasoftware's Adaware](#) - Adaware is the other most commonly recommended anti-spyware tool. Adaware's personal edition is free for non-commercial use.

Download and install the package of your choice. Now. Before you forget.

2. Update the Spyware Database

Your first step should be to update the spyware database that came with the installation. New spyware is being created every day, and databases the anti-spyware programs use are being updated as well. You need to get the latest database for your anti-spyware program right away.

Most of the programs have update functions that will locate, download, and install the latest databases automatically. Microsoft's anti-spyware program will do it automatically for you.

3. Run Regular Scans

Some of the anti-spyware programs don't work automatically - you have to run scans regularly yourself. Do it at least weekly. Use that as an opportunity to make sure that the databases is updated as well.

If your scanner supports scheduling, as some do, make sure to set that up so that the spyware scans happen regularly.

Additional Notes

Some programs support advanced forms of protection that can prevent spyware from installing. For example they may lock your browser home page so that it cannot be changed, or can't be changed without your approval. These techniques are very valuable, and I recommend turning them on.

Sadly, there is no "best" anti-spyware program. Each of them will miss some spyware that the others catch. That's one of the reasons I list several. The best advice is to use one, any one, and have the others "on call" for those cases when spyware sneaks past the one you use regularly.



So just how sneaky can spyware be?

I was asked the following question:

Suppose someone had an MSN instant message conversation on a computer that had spyware on it (unbeknownst to them). Could a hacker access these messages, without access to the computer that had the spyware on it, where the messages were sent from? In other words, from an unrelated computer source?

The scenario you outline is a little unclear, but the short answer is probably ...

Yes

Most of what we call spyware is relatively benign. Annoying and intrusive, but not particularly malicious.

Then there's the other kind.

To get to your question, it is very possible that spyware could, while you are conversing in an instant messaging program:

- Write your conversations to a hidden file and leave open a "back door" that allows the hacker to retrieve that file at a later date.
- Intercept everything you type and everything you receive, and send a copy to another computer somewhere else on the internet as you type it.
- Or any of a number of other things...

Ask Leo! - Good Spyware?

There are commercially available packages that can be used by parents to monitor or control their children's internet use. Is it spyware? Technically yes. It could be used to do exactly the types of things we're talking about here. On purpose. [How can I keep my kids safe from internet garbage?](#)

As you can see, it's just another reason keeping your machine safe from spyware and other malicious software is so incredibly important.



5. Stay Up-To-Date



© [Lincolnrogers](#) | Dreamstime.com

I'd wager that over 90% of virus infections *don't have to happen*. Software vulnerabilities that the viruses exploit usually already have patches available by the time the virus reaches a computer. The problem? The user simply failed to install the latest patches and updates that would have prevented the infection in the first place. I still see this constantly, as some of the most popular articles on Ask Leo! deal with exploits that were patched nearly 2 years ago. The solution is simple: enable automatic updates, and visit [Windows Update](#) periodically.



How do I make sure that Windows is up-to-date?

It seems like every week there's news about some newly discovered vulnerability or bug fix in Windows. And of course the stories tell us that we should all rush out and install the fixes immediately or the world will come to an end.

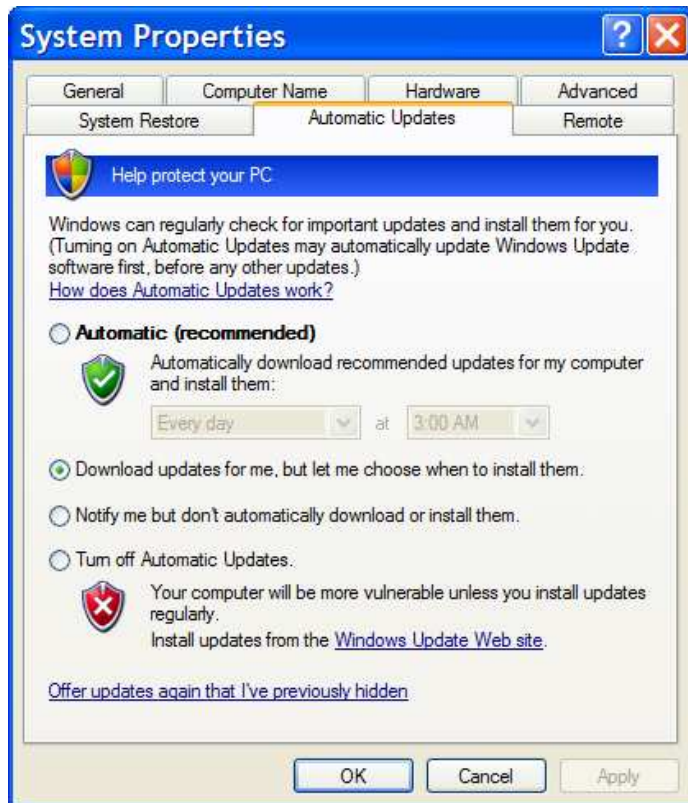
Or something like that.

In fact, Microsoft does announce updates regularly. How should you stay on top of things and make sure that your system is up to date?

There are two answers.

For Windows XP and later, Microsoft created a service that runs on your machine and - on terms you can control - checks for updates to Windows automatically and can download and install them for you.

To configure automatic update, right click on **My Computer**, select **Properties**, and click on the **Automatic Updates** tab. Make sure it's turned on by ensuring there's a check mark in the box where it says "Keep my computer up to date." You have three options controlling how Automatic Update works:



- **Notify on everything** - with this first setting, Automatic Updates will only check the Microsoft web site for updates, and if there are any that apply to your machine, it will alert you, and nothing more. You can then choose to download and install, or not.
- **Notify after download** - with this approach, Automatic Updates will check the Microsoft web site for updates and actually download any that apply. Once downloaded, you're notified that they're available and can initiate the install.
- **Notify after install** - finally, you can just have Automatic Updates do it all, on a schedule you can define. Check, download, and install as soon as updates are available.

For what it's worth, I like to know what's happening to my machine(s) before it happens so I select the second option.

Many people find the concept of Automatic Updates a little too spooky or intrusive. Others just want to have even more control over exactly what happens when. And of course there are folks who are using older versions of Windows. For all these people there's the [Windows Update](#) web site.

The first time you visit Windows Update, it'll download a component onto your machine that handles the inspection of your current Windows component versions. That list is then compared against the latest releases and you'll be informed of the differences. You can then select which components to install.

One important difference is that Automatic Updates focuses on Critical Updates only - those issues that typically represent security or other risky issues. Windows Update, on the other hand, includes both Critical Updates and other updates including newer versions of components and device drivers.

For that reason I recommend that *everyone* visit Windows Update periodically.



6. Get Educated



© [Voitechvik](#) | Dreamstime.com

To be blunt, all the protection in the world won't save you from yourself.

- Don't open attachments that you aren't *positive* are ok.
- Don't fall for phishing scams.
- Don't click on links in email that you aren't *positive* are safe.
- Don't install "free" software without checking it out first - many "free" packages are free because they come loaded with spyware, adware and worse.
- When visiting a web site, did you get a pop-up asking if it's ok to install some software you're *not sure of* because you've never heard of it? *Don't* say "OK".
- *Not sure* about some security warning you've been given? *Don't* ignore it.
- Choose strong passwords, and don't share them with others.



Phishing? What's Phishing?

Phishing is a word you hear a lot in the news these days. This question brought it to mind:

I've received an email from "suspend@msn.net" asking for billing details and threatening the end of my MSN service. Contacting MSN resulted in referral to a support alias, but no answer. Is this a problem, or a forgery?

Well, you're right to be suspicious.

This definitely sounds like a phishing expedition.

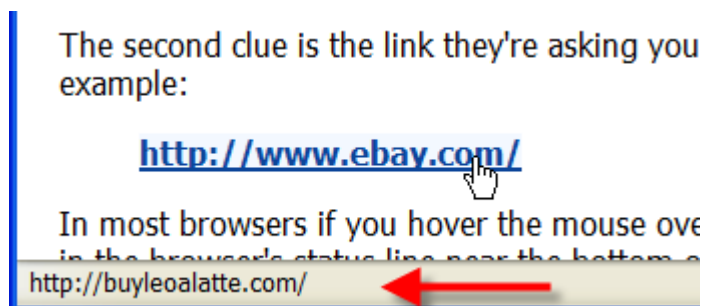
Phishing is very much like fishing, except that you're the fish and that threatening email is the bait. If you bite, you run the very real risk of identity theft and all the hassle that entails.

What happens is this: phishers create email that looks VERY much like an official email from some important entity, like eBay, MSN, Paypal, or perhaps a bank. The email asks you to visit some site, which again, looks very official and proper. There you're then prompted to enter all your personal information again in the guise of "verification".

The problem is that you've just handed over all your personal information to a thief.

The single biggest clue is simple: legitimate businesses simply shouldn't, and the majority don't, ask you for your private information via email. Ever.

The second clue is the link they're asking you to click on. It may *look* like it links to eBay, but in fact it goes somewhere else entirely. Here's an example:



In most browsers if you hover the mouse over that link on a web page, you'll see that it does *not* go to eBay, (you'll see the real destination either in popup text, or in the browser's status line near the bottom of the window as shown above). But it looks like it does. If you click on it, you'll be taken somewhere else entirely. The same tricks work in HTML formatted email, which is what most of these phishing attempts use.



Now, in the example above, it's obvious you're not at eBay if you click through. But if the destination site *looked* like eBay, you could be fooled into thinking it was legitimate.

So if you're tempted at all, hover your mouse over the link, and *look before you click!*

The actual destination should match what you expect. *Exactly*. If the link claims to be eBay, <http://ebay.hacker.com> is *not* where you want to go. Nor is <http://www.ebay.cc> (note that it's not ".com"). In the original question, "msn.net" as a return address is not the same as "msn.com". That's a big red flag.

The actual destination should be a name, not a number. If the destination of the link takes you a link that has numbers, such as <http://72.3.133.152>, chances are it's not valid.

The actual destination should probably be secure. That means it should begin with **https:**. If the target destination begins with the regular, unsecured **http:**, chances are it's not legitimate.

The single, most important rule regarding these emails is simple: if they provide a link to click on, ignore them. **Never** click a link in the email itself.

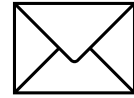
If you *must* satisfy your curiosity, then *type* what you know to be the *correct* URL into your browser by hand, and login to your account as you normally would. If there's something you need to do or verify, then you'll probably see it then.

And if you're still not sure, then give the institution a call. Trust me; they'd rather have you ask than have to deal with the possibility of identity theft.



How do I get rid of all this spam?!?!

If it seems like it's been getting worse lately that's only because it has. The amount of spam has only been increasing, and latest attempts to legislate a solution appear to have had little if any impact.



So what's a poor user to do?

The unfortunate bottom line is that there is no magic answer and no silver bullet. There is no solution today that will guarantee you get only the email you want while also guaranteeing you get all the email you want. There are many partial solutions that have varying degrees of success, depending on your needs and your willingness to accept some of the restrictions or some additional steps.

Email filters work by analyzing your email's contents prior to your seeing it and then flag or delete the email that it thinks is spam. You can probably guess the problem with most filters - sometimes they guess wrong. It's typical to continue to receive a reduced number of spam emails even with filtering in place. What's worse is that filters will occasionally mark as spam email that you truly wanted. In a business situation this is simply unacceptable. The good news is that most spam filters are "tunable" - meaning that you can adjust how aggressively they filter spam.

I don't have any formal recommendations for spam filters. Not because there aren't good ones out there, but because they are very specific to either your email server or ISP or to your email client. I will note that many of the more popular filters are based on [SpamAssasin](#) technology. Also, my wife and I have recently been having very good results with Microsoft Outlook's junk mail filter.

If you can't use a filter, what then? The most common solution is to have multiple email addresses. One approach is to select one to be your "private" guarded email address - much like an unlisted phone number - that you never use in situations where the email address would be harvested for spam mailing lists. The other approach is to generate "throw-away" email addresses that you use only for a limited time (say when registering a product), and can safely ignore thereafter. And of course both approaches can be used at the same time.

A recent entry into the fight against spam is something called challenge/response. It's available as a service from various companies and is now also sometimes offered or required by some ISPs. Challenge/response as its name implies is a challenge sent in response to



email from an unknown source to prove that the sender is human. If they respond and confirm that they are, a) they are remembered and never have to see a challenge again, and b) the mail they sent you is delivered. If they do not respond then you never see the email.

The problem with challenge response relates to any mailing list you might sign up for, any on-line purchase that might result in sending you an email confirmation, or any legitimate organization that might send you valid yet automated email. This is email you want. Yet senders to such lists do not have the time or the resources to respond to a challenge for each of their recipients. Typically they'll simply ignore all challenges. The result: unless you remember to proactively white-list them beforehand then you won't get the email you request.



7. Secure Your Mobile Connection



© [Cyrano](#) | Dreamstime.com

If you're traveling and using internet hot spots, free Wifi or internet cafes, you *must* take extra precautions. Make sure that your web email access is via secure (https) connections, or that your regular mail is over an encrypted connection as well. Don't let people "shoulder surf" and steal your password by watching you type it in a public place. Make sure your home Wifi has WEP security enabled if anyone can walk within range.



How do I stay safe in an internet cafe?

Anyone within wireless range of your laptop could be monitoring your internet usage.

Scary, huh?

Here's what you need to do:

Use a firewall! You may already be doing this, but this is critical. And it doesn't have to be difficult; for example I simply enable the Windows firewall when I'm in an open WiFi situation.

Yes, there may be a router or firewall at the hotspot protecting you from threats from the internet, and that's fantastic. It's also not at all what I'm talking about here. In an open WiFi situation and in any "internet provided" situations like hotels you need to protect yourself from everyone else that's on the same side of the router as you are. They can see and connect directly to your machine unless you enabled your firewall.

Use httpS! That's https, note the "s" at the end. An https connection is encrypted. That means that while someone can see that you're accessing a particular web site, if you're using https they cannot see any of the data you send to or receive from that site. This is the only safe way to do online banking. If you can't connect via https, or the "s" disappears at some point in your exchange with your bank, then stop. If it's not https, it's not secure and anyone in the room could be monitoring what you're doing.

Secure your Email! Email is perhaps the biggest open security hole in these situations. If you use a POP3/SMTP email client, the default configuration for most is totally unsecure. I could sit in a corner of the internet cafe and not only read your email with you, but also steal your account name and password. It really is that unsecure.

Ask Leo! - Trust your ISP?

Your ISP can monitor everything you do. I'm not saying that they do, but they can.

When you're using a wireless hotspot such as in an internet cafe, *they* are your ISP for that connection. Again, I'm not saying that Starbucks or their wireless provider is spying on you, but I would take care to make sure you trust the provider you're using. If you're at "Joe's Cafe" and it's Joe's teenage son that's just slapped a wireless access point on their DSL connection - yes, he could be monitoring what you're up to.

But that's not really the biggest threat. The people we shouldn't trust are the other users nearby, within range of that wireless connection.



With POP3 and SMTP you should contact your email provider and see if they support SSL connections. If they do, it's a slightly different configuration in your email program but once done all of the communication between your email program and email servers are securely encrypted.

Online or web-based email services deserve special consideration. Most do not support https connections. The one exception is Gmail, which will use https if you make sure to login through an https connection.

Consider a VPN. Not all sites support https, as it takes extra work on their part. For example there is no https version of ask-leo.com, you can only access it through unencrypted http, and that's the norm for most sites that don't process confidential information. But that means that someone could still be watching where you go. If you don't mind them seeing that you're visiting ask-leo.com, or what you might happen to search for on Google, or whatever other sites you're visiting in the clear, then you don't need to do anything.

And not all email providers will provide secure connections.

However, if you're a "road warrior" and spend a lot of time in internet cafes, have an unsecure email configuration, or browse a lot of sites that you'd rather not be so easily sniffable, you might consider a VPN (Virtual Private Network) service. I've never used one personally, so I can't recommend one specifically but there are several. [HotspotVPN](#) is just one example. Using these services you create an encrypted connection to the service and route all your internet traffic through them. When you do this the folks in the cafe see only encrypted data which they can do nothing with.

So, how big is the risk, really?

It depends.

I'd expect busy hotspots near sensitive areas to run a fairly reasonable risk. Busy coffee houses, airport WiFi, libraries and the like seem like "target rich environments" for the potential hacker. These are certainly places where I'd make sure to take these safety measures myself.

Less busy hotspots? Perhaps not so much.

But it is possible, and more frighteningly, it's not all that hard for someone who's technically savvy.

And every time you use public internet facilities and hotspots, you may be at risk.



Can hackers see data going to and from my computer?

Yes.

But *most* of the time it doesn't matter. On the other hand, there are times when you really need to be careful.

Data traveling on a network such as the internet can be seen by many other machines. Local machines connected via a hub, for example, all see the data being sent to and from all the other machines connected to the same hub. As the data travels the internet, it's quite possible that other machines on the network can also see the data.

Sounds scary.

The good news is that it's really hard to find data transmitted to and from a *specific* machine unless you're on the same network segment. For example if you're connected to the internet via DSL, other machines sharing your DSL could watch your traffic, but machines out on the internet would have an extremely difficult time tracking it down.

It's not something I worry about much.

However, there *is* a scenario that you should be very aware of.

Wireless network access points operate much like a hub. Any wireless adapter in range can see all of the network traffic in the area.

Visited any wireless hotspots lately? Anyone in the coffee shop, library, other public places, or even just outside on the street or a nearby building could be sniffing your traffic.

So, what to do?

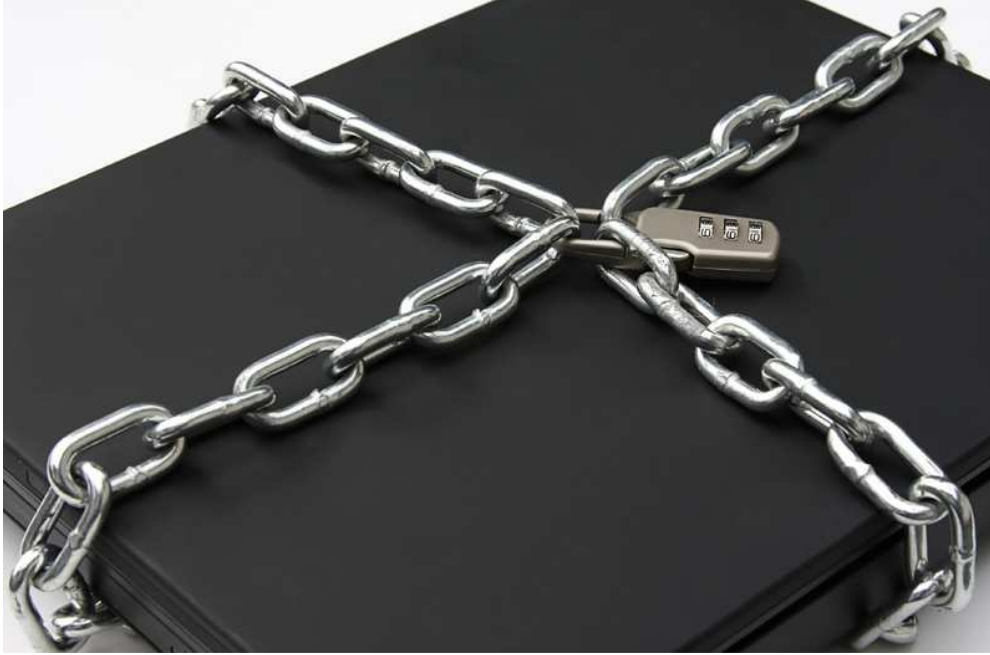
Well, for one thing, make sure that any sensitive web surfing you might choose to do - such as banking or on-line shopping - is always done via a secure connection. Even better - wait until you're home to do those things.

Email is particularly sensitive. For example it's not difficult to sniff your email account information when downloading email via a normal POP3 account, or sending via SMTP. Web interfaces that use "https" secure connections are actually safer.

And if your wireless network at home is within range of other houses, the street, or other public areas, make sure you're at least using 128bit WEP to ensure that the data that would be visible is encrypted.



8. Don't forget the physical



© [Stevebyland](#) | Dreamstime.com

An old computer adage:

If it's not *physically* secure, it's not secure.

All of the precautions I've listed above are pointless if other people can get at your computer. They may not follow the safety rules I've laid out. A thief can easily get at all the unencrypted data on your computer if they can physically get to it. The common scenario is a laptop being stolen during travel, but I've gotten reports of people who've been burned because a family member or roommate accessed their computer without their knowledge

How can I keep data on my laptop secure?

I have sensitive information on my laptop that I would prefer not to fall into the wrong hands. I can handle losing the laptop, but the thinking about the data in the wrong hands ... well, it just gives me the willies.

So, yes, I do have a solution, and it turns out to be fairly easy, secure, and free.

Now, naturally, you can "encrypt" your data using a simple tool like WinZip and assigning the resulting archive a password. The problem is that it's fairly easy to crack the zip file's password, and get at the data. It has its uses, though. Much like a cheap padlock, it's mostly about keeping honest people honest.

I recently started using something called [TrueCrypt](#). TrueCrypt is free, open source, on-the-fly encryption software. It provides serious industrial-strength encryption while still being fairly easy to use.

The logo for TrueCrypt, featuring the word "TRUECRYPT" in a blue, sans-serif font on a dark blue rectangular background.

TrueCrypt can be used in several ways, the two most common are that it can encrypt an entire disk volume - such as a USB thumb drive, floppy disk, or an entire hard disk if you like - or, it can create an encrypted virtual disk. It's this later approach that I like to use.

An encrypted virtual disk is simply a file that TrueCrypt "mounts" as an additional drive letter on your machine. You specify the pass phrase when the virtual drive is mounted and thereafter everything you access from there is automatically *DE*ncrypted and anything you place there is *EN*rypted.

For example, you might have TrueCrypt create an encrypted drive as **c:\windows\secritstuf**. If someone were to look at the contents of that file directly, they would see only random gibberish - the result of encryption. When using TrueCrypt to mount that file as a virtual drive, (for example selecting the drive letter "P:") then P: would look and operate like any other disk, and would contain the contents of the encrypted drive. Encryption is as simple as moving a file to the drive.

The trick, then, is to never mount the drive automatically. When your machine boots up, "P:", for example, would be nowhere to be found, and the encrypted file c:\windows\secritstuf would be present, but only visible as gibberish. If someone stole your machine that's all they would find.

Only after you've used the TrueCrypt program to select the file (c:\windows\secritstuf), choose the drive to mount it as (P:) and supply the correct pass phrase, would the virtual drive be "mounted" and the encrypted data become accessible.



TrueCrypt supports a number of different high-powered encryption algorithms. The documentation for TrueCrypt is clearly targeting at the seriously paranoid, including instructions on how to maintain "plausible deniability" should a thief ever force you to supply a password. Let's hope that'll only be of passing interest to any of us.

Now, a couple of caveats:

Encryption does not make a bad password any more secure. If you choose an obvious password or pass phrase, a dictionary attack can certainly be mounted that could unlock your encrypted volume.

An encrypted volume does you no good if the files you care about are also elsewhere on your machine.

That being said, make sure you have secure backups, updated regularly. Preferably keep them UNencrypted, but secure in some other way, in case you lose your encrypted volume or forget your password. Without the password, the data is **not** recoverable.

That last statement is technically inaccurate. You should always be aware that things are *never* 100% secure. All encryption can, *theoretically*, be hacked. The purpose of encryption is to make the cost of that hacking so astronomical as to be impractical. For example, spending a calendar year on a brute force hacking attempt is kind of pointless to discover next month's sales forecasts. Similarly hiring the expertise required to attempt such a recovery might also be astronomically costly.

Data encryption is an important part of an overall security strategy. Keeping your sensitive data secure requires a little forethought and planning. With viruses and spyware running amok, not to mention the theft scenario that we started this article with, there's no excuse not to take that time, and save yourself some serious grief later if the unthinkable happens.



What backup program should I use?

Doing backups is kind of like eating healthier; everyone agrees we should and yet very few of us actually do. Much like the heart attack victim who no longer visits McDonald's the most religious users of backup procedures are those who've been bitten hard by a failure in their past.

Asking what backup program to use is very much like asking "what's the best exercise program?" The best program for exercise or backup is whatever one you'll actually *do*.

Do you know how you'd recover your data should your computer crash?

In order to choose what's right for you, there are several questions you should be asking yourself.

- **Do I want to put a lot of thought into this?** If not then prepare to spend a little more money for some additional disk space and get one of the stock backup programs. I'm currently quite pleased with my external [USB/Firewire Maxtor](#) drive and while I run my own custom backup (more on that below), it comes with [Retrospect](#) which is a respected backup package.
- **Am I comfortable re-installing my system if something goes wrong or do I want the backup to take care of that?** This is one of those comfort versus space tradeoffs. If you're ok with re-installing your system, and that means your operating system as well as applications and customizations and you can clearly identify what does and doesn't need to be saved, then you can save a lot of disk space by backing up only your data. This requires some amount of diligence on your part because anything you don't specify to whatever backup program you use will be lost in the case of a catastrophic failure.
- **Is there another machine nearby?** Quite often you don't even have to go out of your way to get additional hardware for backup purposes. Hard disks are so large these days that quite often simply having another machine on your network with sufficient free space can be a quick and easy solution. Many backup packages will allow you to backup across a network. Having two machines each back up to the other is a quick way to ensure that if either has a problem your data is safe on the other.
- **How valuable is what you're doing?** As much as we hate to think of it we should: what if your building including your machines and all their backups were lost in a fire? If the potential data loss just sent a shiver down your spine then you should be considering off-site data storage for your backups. That could mean burning a CD or



DVD periodically and leaving it at some other location or if the sizes are small enough or backing up across the network to some server not in your home.

- **How important is incremental access?** By incremental access I mean; how important is it that you be able to recover a file from a specific day and not a day before or after? If you simply back up all your files on top of previous versions you'll only have the most recent version. In many many cases that's enough. In some cases it's not such as needing to recover an older version of a file that became corrupt at some point.
- **What resources should I backup?** Have you thought of all your computers? All the drives therein? How about external hard drives you're not using for backup? Do you have a web site? Do you have a backup of it? What would happen if your ISP "lost" it? (It's happened.) If you're a small business, do you have databases that need backing up? Office machines that belong to everyone but no one?

Let's use myself as an example for those questions:

I've put *a lot* of thought into this. And I should; it's my profession to do so and my business relies on it. In my case I use my own scripts written in Perl and leveraging a tool I wrote many years ago called [SyncFile](#).

I'm very comfortable re-installing everything so I backup only my data. Even so, just last week I discovered an overlooked directory that cost me a couple of hours time when I had to reconstruct a missing file. That directory is now part of my backup. Am I missing more? I hope not.

I have several machines on my LAN in the middle of the night there is a flurry of activity as data gets copied from one machine to another and another, each using at least one other as a backup.

What I do for my business is definitely valuable and worthy of off-site backup. My solution is actually fairly simple - with computers at two different physical locations I have two external [Maxtor](#) drives - each location backs up to the external drive and roughly once a week we swap the drives.

I do have external servers as well. For example the web site hosting [Ask Leo!](#) resides on a server hundreds of miles from my office. So I've been careful to ensure that it too is backed up in some appropriate way.

The bottom line for backup is simple: just do it. Understand what you have and what you're willing to invest in but do something.

Before it's too late.

That's It, And Yet...



© [Lisafx](#) | Dreamstime.com

We've covered the basics, from firewalls and malware protection, to basic education and even understanding the risks associated with anyone being able to reboot your computer.

It's a great foundation, a good beginning, but in reality ...

It's only a start.

Things are changing every day. New tools, new threats and new situations are showing up all the time. I don't want to sound like an alarmist, because I'm not really, but it's important to build on what you've learned here and stay aware of what's happening as you continue to use your computer and the internet.

In fact, I hope you'll take advantage of the many resources out on the internet. Yes, of course I'm particularly hopeful that you'll come visit <http://ask-leo.com>, perhaps even sign up for my [free weekly newsletter](#) - but even if you don't, realize that a lot of information is out there, and there are a lot of folks out there just like you who are looking for, and giving back, great help and advice.

And as for me? Well, you know where to find me. Drop me a line, or a question, any time...

A handwritten signature in black ink, appearing to read 'Leo'.

Leo A. Notenboom
<http://ask-leo.com>

