Ask Leo!
by Leo Notenboom

INTERNET SAFETY

Keeping Your Computer Safe on the Internet

LEO A. NOTENBOOM

http://ask-leo.com

Internet Safety

Keeping your Computer Safe on the Internet

3rd Edition

by

Leo A. Notenboom

http://ask-leo.com

ISBN: 978-1-937018-03-0

Copyright and Disclaimer

Having said that, the PDF electronic version (only) of this book is ***FREE***. In fact, I encourage you to **share this book** with others as long as you share it:

- In its entirety (the book, the whole book and nothing but the book)
- In its original form (no changes made and no markups added)

You may not charge for this book when you share it. Furthermore, you may not incorporate this book into any product or collection that is not free. (Drop me a line for pricing if you want to do something along those lines.)

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. ☺

Table of Contents

Viruses & Spyware & Worms ... oh my! 8
Security Software 10
What security software do you recommend? 11
The Short-Short Version 11
Microsoft Security Essentials 12
Other Good Alternatives 12
Malwarebytes 13
Anti-Virus 13
Anti-Spyware 13
Firewall 14
What Else? 14
Related Articles on Ask Leo!: 14
Scan for Viruses 16
Viruses: How do I keep myself safe from viruses? 17
Install and Run an Anti-Virus Program 17
Update the Anti-Virus Database 18
Run Regular Scans 18
Keep Windows Up-To-Date 18
Additional Notes 19
Related Articles on Ask Leo!: 19
I run anti-virus software, why do I still sometimes get infected? 20
The Race - And Bad Luck 20
All Anti-Virus Software is the Same, Only Different. 21
The Internet - Wear Protection Before Touching It 21
The Harsh Reality 21
Why? 22
Related Articles on Ask Leo!: 22
When do I actually need to run a virus scan? 23

Real-Time 23
On-Demand 23
Which? 24
Updates 24
Related Articles on Ask Leo! 24
What's wrong with scanning email in real time? 25
Real Time Email Scanning 25
Real Time Email Destruction 25
The Alternatives: Common Sense and On-Demand scanning 26
My Recommendation 26
Related Articles on Ask Leo! 27
Kill Spyware 28
How do I remove and avoid spyware? 29
1. Install and Run an Anti-Spyware Program 29
2. Update the Spyware Database 30
3. Run Regular Scans 30
An Additional Recommendation 30
Some Additional Notes 30
Related Articles on Ask Leo! 31
So just how sneaky can spyware be? 32
Related Articles on Ask Leo! 33
Use a Firewall 34
What's a firewall, and how do I set one up? 35
Network-based threats 35
Hardware firewalls, like your router 36
Software firewalls 36
Choosing and setting up a firewall 37
Firewalls are only a part of the solution 37
Related Articles on Ask Leo! 38
Do I need a firewall, and if so, what kind? 39
Related Articles on Ask Leo! 41
Does my router have a firewall or not? 42

Related Articles on Ask Leo! 44
Is an outbound firewall needed? 45
Related Articles on Ask Leo! 47
So do I need the Windows Firewall or not? 48
Related Articles on Ask Leo! 49
How do I change my router's password? 50
Related Articles on Ask Leo! 54
How do I secure my router? 55
Change The Default Password 55
Disable Remote Management 56
Turn Off Logging 56
Add a WPA Key 57
Don't Forget The Physical 58
Related Articles on Ask Leo! 58
Stay Up-To-Date 59
Are automatic updates a good thing? 60
Related Articles on Ask Leo! 61
How do I make sure that Windows is up-to-date? 62
Related Articles on Ask Leo! 64
Get Educated 65
What's a good password? 66
What's a bad password? 66
What's a good password? 67
The compromise 67
Using Technology 67
Related Articles on Ask Leo! 68
How long should a password be? 69
Large scale account hacks 69
Dictionary attacks 70
Brute force attacks 70
Why 10 is better and 12 better still 71
What about special characters? 71

Related Articles on Ask Leo! 72
Phishing? What's Phishing? 74
Related Articles on Ask Leo! 76
Is changing my password enough? 77
Related Articles on Ask Leo! 79
Backing Up 81
What backup program should I use? 82
Related Articles on Ask Leo! 84
How did you backup while on your trip? 86
External Hard Drive 87
Postal Mail 87
A Note About Sequencing 88
A Note About Security 88
Are You Protected? 89
Related Articles on Ask Leo! 89
Secure Your Mobile Connection 91
How do I use an open WiFi hotspot safely? 92
Turn On The Firewall 92
Consider Not Using Free WiFi 93
Secure Your Desktop Email Program 93
Secure Your Web-based Email 94
Use a VPN 95
Use Different Passwords 95
Related Articles on Ask Leo! 95
Can hotels sniff my internet traffic? 97
Related Articles on Ask Leo! 99
Can hackers see data going to and from my computer? 100
Related Articles on Ask Leo! 102
Don't forget the physical 104
How can I keep data on my laptop secure? 105
Related Articles on Ask Leo! 107
Will using an on screen keyboard stop keyboard loggers and hackers? 108

Related Articles on Ask Leo! 110
That's It, And Yet... 111
About the Author 112

Viruses & Spyware & Worms ... oh my!

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 and irresistible target for hackers and "script kiddies".

In this book I'm 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:

- Security Software - We'll start with a quick overview of the software that I suggest as at least part of keeping your computer safe on 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.
- 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.
- 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.
- Backups - No book on internet safety would be complete with at least an overview of the single most effective way to recover from safety disasters.
- 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 book is based on articles 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.

I'm giving the downloadable version 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.

And once you're done, I'm hoping you'll realize that these topics are so important, and so easily overlooked, that you'll share this book - and Ask Leo! itself - with your family and friends.

Security Software

One of the more common questions I get is exactly what security software I use and recommend. That's changed as security software comes and goes and as newer packages mature and older ones fall out of favor. Here's an article that wraps up all the recommendations in a single place.

What security software do you recommend?

I have recommendations for specific products in various places on the site. Here's a short single page summary.

What anti-virus software should I use? How about a firewall? And what about spyware? Should I use one of the all-in-one packages that claim to do everything? Anything else I need?

•

As you might imagine, I get these questions in various forms all the time. As a result, I do have recommendations in various articles all over Ask Leo!.

Here's the short version that sums it all up.

•

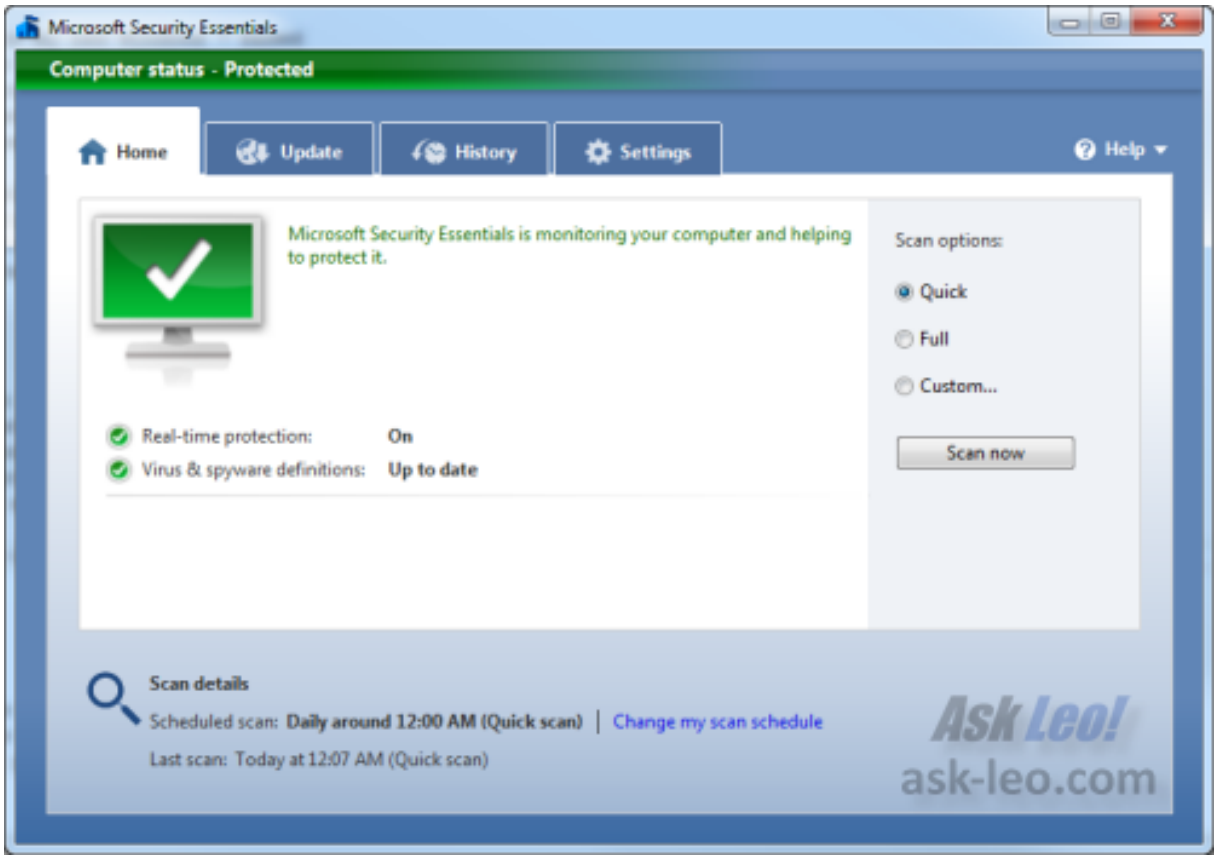
The Short-Short Version

Here's my current recommendation for most home and small business users who don't want to think about it too much:

- Get a router which will be your firewall, even if you have only one computer.
- Install Microsoft Security Essentials as your anti-virus, anti-spyware and malware scanner.
- Turn on Windows Automatic Update.
- Turn on the Windows Firewall when you travel.

That's it. Good, basic protection in four steps with only one download.

Microsoft Security Essentials



In the past, I've strongly disrecommended all-in-one solutions. By "all-in-one" I mean a single program or "security suite" that claims to do it all: firewall, anti-spyware, anti-virus and often much more all in package. What I see in reports and questions coming in to Ask Leo! is simply this: these types of suites typically have or cause more problems than other alternatives.

That strong disrecommendation continues - I've not changed my mind.

With one exception: Microsoft Security Essentials.

In a sense, it's not an all-in-one solution like the others. True, it has anti-virus and anti-spyware but where it differs is that it's not trying to shovel in all sorts of other features that a) you don't need and b) often only serve to destabilize your computer. Microsoft Security Essentials isn't trying to compete against other products long feature list - and as a result it wins.

Other Good Alternatives

Microsoft Security Essentials might not be the right solution for everyone. No single product is.

In addition, even with a good, solid foundation you may also find yourself needing additional tools at times. The unfortunate but very practical reality is that no single tool or combination of tools can find all malware all the time. As a result, you may sometimes need alternatives to bring in to help out.

Malwarebytes

I throw Malwarebytes Anti-malware into a classification by itself. It's not really an anti-virus tool, per se (in fact in their forums you'll see the support staff regularly recommending anti-virus tools to install alongside Malwarebytes), and I can't really call it an anti-spyware tool either.

But is currently has one of the best track records of removing troublesome malware quickly and effectively.

Hence anti-malware.

Malwarebytes' Anti-Malware comes in two versions: free and pay. The free version is a fully functional stand-alone manual scanner. The paid version adds realtime scanning, and scheduled scanning and scheduled updates.

Anti-Virus

AVG Free and Avira Free are two free solutions that I've come to recommend. I ran AVG for some time on my primary machine, Avira protected my wife's for a long time as well.

I have two concerns with both:

- When you visit their site and download the program, they both try really, really had to up-sell you to the paid versions. Be persistent, be careful, and make sure you get the free version - it's the free version that I'm recommending here.
- AVG Free includes a feature called "LinkScanner" that attempts to check links on the pages of the sites you visit for phishing and other malware. I've experienced and also had several reports of this feature seriously impacting browser performance. I recommend turning it off immediately. In fact, I recommend turning off any browser intrusive or email intrusive features on any anti-malware program at the first sign of problems.

Anti-Spyware

Spybot Search and Destroy is one of the longest running and highly regarded anti-spyware tools out there. I wouldn't hesitate to install and use it.

Also one of the "old guard" is Lavasoft's Ad-Aware. It's had some issues in years past but as I understand it it's a solid contender once again. My only

concern with Ad-Aware is that being a commercial product (though with a free version) it does seem to be starting down the road of perhaps trying to do too much.

Firewall

For home & business use I recommend the use of any good NAT router as a firewall. They don't have to be expensive at all, and are one of the simplest approaches to keeping your computer safe from network-based threats. If all the computers on the local network side of the router can be trusted, then no additional software firewall is called for.

When traveling, I recommend simply turning on the built-in Windows Firewall. (There's often no harm in leaving it on at home, but it can occasionally get in the way of some local machine-to-machine activities.)

I understand that some people feel strongly that an additional software firewall is still called for in certain circumstances, but in my opinion those circumstances are infrequent. I do not have a specific product to recommend, as all of the current software firewalls seem to cause issues, often serious, from time to time.

What Else?

I strongly recommend you backup, regularly. In fact I can't stress this enough. 99% of the disasters I hear about could be completely avoided simply by having up to date backups. Acronis TrueImage is the backup software I use and recommend.

Keep your computer up to date. That means turning on Windows Update or making sure to visit the Windows Update web site religiously. The vast majority of computer infections we hear about are due to the operating system simply not being kept up to date with the latest available patches.

Related Articles on Ask Leo!:

- With Microsoft providing Microsoft Security Essentials do I no longer need to purchase malware protection? Microsoft Security Essentials provides basic anti-virus and anti-spyware scanning for free. It appears to be a reasonable anti-malware tool for many.
- Viruses: How do I keep myself safe from Viruses? Computer viruses are a fact of modern connected life. Anti-virus software is required, and both it and the database it uses should be kept up-to-date.
- Do I need a firewall, and if so, what kind? Firewalls are a critical component of keeping your machine safe on the internet. There are two basic types, but which is right for you?

- Spyware: How do I remove and avoid spyware? There are some important steps to take to deal with the ever-present concern of how to remove and avoid spyware.

Article C3517 – August 14, 2010

Scan for Viruses

Sometimes, typically via email, viruses 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 viruses 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 connected life. Anti-virus software is required, and both it and the database it uses should be kept up-to-date.

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, and perhaps your bank account or identity, goodbye.

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

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

•

Install and Run an Anti-Virus Program

There are many out there.

From my article What Security Software do you recommend?, the super-short version is to install Microsoft Security Essentials. This is what I currently run on all of my machines.

I also run Malwarebytes Anti Malware periodically. This is what I use when I remove viruses from friends' machines. After some recently pervasive virus infections, it was one of the first to recognize and clean them up. It has also garnered quite a good reputation.

I've run other anti-virus solutions with good results including the free versions of AVG and Avira. I also hear good things about the free version of Avast.

While I'm not a big fan of their product offerings, Symantec maintains one of the best reference sites for virus related security issues.

Not all virus scanners catch all viruses. I recommend having a selection of additional virus scanners to run as a "second tier". Most downloadable virus scanning solutions often include free trial periods that can also come in handy as one-time second-level scans.

Whatever it is you choose, download and install the package of your choice.

Now. Before you forget.

Update the Anti-Virus Database

After installing your anti-virus software, your first step should be to update the virus signature database that came with it.

The anti-virus program alone isn't enough. Each uses a database of known viruses to know what to check for and that database needs to be kept up-to-date.

New viruses are being created every day and the databases used by anti-virus programs are being updated that frequently as well. You need to update to the latest database for your program right away.

Most of the programs have update functions that will locate, download and install the latest databases regularly and automatically.

Make sure that this is enabled.

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. (There are scenarios where real-time scanning, particularly of email, may cause problems. Unless or until you run into those problems, however, you should leave this enabled.)

I also recommend periodically running scans of your hard disk, including all hard disks if you have more than one. 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.

Keep Windows Up-To-Date

Visit Windows Update regularly, or simply enable the automatic update feature in Windows.

All software has bugs. Some of those bugs result in vulnerabilities that are then exploited by malware writers to create viruses that can infect your system. As these bugs are found, Microsoft fixes the affected components in the operating system, eliminating the vulnerabilities, and makes those fixes available for download and automatic installation 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.

Don't be one of those people.

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.

Additional Notes

There is no "best" anti-virus program.

In fact, any measurement of which are "better" or "worse" changes over time. Each may miss something that the others catch. That's one of the reasons why I list several alternative anti-virus programs above. The best advice is to use one, any one, and have the others "on call" for those cases when a virus sneaks past the one program that 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, as they say, "unpredictable results".

Related Articles on Ask Leo!:

- What Security Software do you recommend? I have recommendations for specific products in various places on the site. Here's a short single page summary.
- How do I remove a virus? Once you've been infected with a virus or other malware, there are steps you can take to try to remove it, but only one approach is guaranteed to work.

Article C2339 - October May 28, 2011

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

> It seems like even the most up-to-date anti-virus software package isn't always enough. It's frustrating, since you'd think that it would be.

I have AVG virus protection always on and windows XP firewall enabled. Why do I still get infected with some Trojan horses? I check for updates every day so I am sure I am up to date.

•

That's a very good question, particularly since so many people believe that with only an anti-virus program they're totally protected.

Unfortunately, that's simply not true.

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 - "the race" - on purpose. Combating viruses is a three way race:

- In the lead are virus writers looking for vulnerabilities and writing viruses to exploit them
- Coming in second are the anti-virus software vendors looking for ways to detect each new virus as it appears as well as figure out the correct way to eradicate it when found
- Next are the software vendors looking to plug the security holes that the viruses exploited in the first place.
- Lastly are folks like you and me: hopefully keeping our systems up to date with the latest updates to both our anti-malware products as well as the systems and software that have vulnerabilities.

As you can see, virus writers are almost always in the lead. You and I? We're dead last. Hopefully close to the pack, but still - last.

As a result the first answer boils down to simple bad luck. It's possible to be doing everything as right as you can and still get infected if:

- your anti-virus software has not yet been updated to know how to detect it

and

- your software has not yet been patched to fix whatever vulnerability the virus exploits

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

Sadly, as far as I can tell, there is no "best" anti-virus or anti-malware package. Most all of the name brands are good, but I've not run into one that really stands out above the crowd at detecting absolutely positively 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 anti-malware tools are completely up to date.

The Internet - Wear Protection Before Touching It

One of the more frustrating scenarios I've seen involves going through great lengths to clear a machine of viruses, only to get infected again within seconds of connecting to the internet.

Some classes of 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.

Firewalls help - particularly hardware firewalls such as routers. 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.

The good news here is that most operating systems now either come with a software firewall turned on by default, or strongly encourage you to turn it on as you perform your initial install.

The Harsh Reality

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, some exist to silently send spam 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.

No anti-malware tool can protect 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.

If you choose to connect without a firewall, or choose not to use automatic updating tools to keep your system as up to date as possible ... it's on you to know what you're doing.

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 that makes for a bigger target, and more. Of late, there's a lot of money to be made by infecting large numbers of machines with spam-sending bot software.

Of course it shouldn't be like this.

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

Related Articles on Ask Leo!:

- Internet Safety: How do I keep my computer safe on the internet? Internet Safety is difficult and yet critical. Here are the seven key steps to internet safety - steps to keep your computer safe on the internet.
- Viruses: How do I keep myself safe from Viruses? Computer viruses are a fact of modern connected life. Anti-virus software is required, and both it and the database it uses should be kept up-to-date.
- Do I need a firewall, and if so, what kind? Firewalls are a critical component of keeping your machine safe on the internet. There are two basic types, but which is right for you?

Article C2175 - January 3, 2010

When do I actually need to run a virus scan?

> There are two types of virus scans: continuous or periodic. Which and how many you need and how often they're needed depends on your situation.

Do you have more than one anti-virus program running at any one time, to stop newly arriving viruses, or do you just have them ready to run when you've got a virus and want to clean it out?

•

Virus scanners are best used to prevent viruses from ever reaching your machine, but you raise a very good issue that most folks don't realize.

There are two types of scans, and each has a place and a purpose.

•

Real-Time

The most common type of scan is the continuous "real-time" scan that watches for viruses in data as it arrives (and possibly as it leaves) your computer. I say it's the most common because it's enabled in the default configuration of most anti-virus programs.

Using a real-time scan, the anti-virus software will hook into your network connection and simply watch the data coming and going to and from your machine, watching for viruses. If it identified one then it takes appropriate action and alerts you.

Typically, real-time scans are considered the safest, since viruses are caught before they've 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 extremely important that there be only one real-time scanner running at a time, as they can conflict with each other resulting in false positives, missed viruses, program crashes or worse. But fortunately one real-time scanner is all you need.

On-Demand

With an "on-demand", or scheduled scan the virus program simply examines the contents of your hard disk, reading the contents of every file looking for viruses. Naturally, reading everything on your hard drive can take a little time.

Free virus scans are often on-demand. You initiate a scan, and a while later the scanner tells you whether or not your machine is infected and whether or not it was able to remove the infections.

When an on-demand scan is complete no further scanning is performed until the next on-demand scan. It runs, scans everything, and then finishes.

Which?

Most anti-virus programs include both types of scans, real-time and on-demand. Most will enable the continuous real-time scans by default, but also offer some form of scheduler so that you can automatically run the on-demand scans.

I typically 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 actually don't run a real-time scan, since I'm fairly well protected in other ways and find that real-time scans can occasionally interfere with the performance of my machine. They've also been known to cause other anomalous behavior - most commonly with email. I do, however, run an on-demand scan which is scheduled every night.

Updates

Regardless of what type of scan you run, it's critical that you make sure that the database of virus definitions your scanner uses is as up-to-date as possible. Most anti-virus programs include a scheduler for that as well, and I make sure that mine is configured to download the latest database every night.

Whether you run a real-time scanner or a nightly or other periodic scan, remember that it's critical to do something. The days of being blissfully ignorant about viruses is long past.

Related Articles on Ask Leo!

- I run Anti-Virus software; why do I still sometimes get infected? It seems like even the most up-to-date anti-virus software package isn't always enough. It's frustrating, since you'd think that it would be.
- What Security Software do you Recommend? I have recommendations for specific products in various places on the site. Here's a short single page summary.

Article C2250 - March 6, 2010

What's wrong with scanning email in real time?

> Scanning your email for malware in real time as it downloads to your machine sounds like a great idea – until you start losing email.

You've said you're not a big fan of real time email scanning ... can you tell me why? Is there another way to scan it?

•

I base that mostly on the problems I see reported here that are solved by turning real-time email scanning off and using alternatives instead.

The tools have certainly gotten better over time, and it does feel like I'm seeing fewer problems, but fewer isn't the same as none at all.

I'll describe what I mean by real time scanning, the problems that it's known to have I've seen it introduce, and the alternatives I prefer.

•

Real Time Email Scanning

To me "real time" email scanning is exactly what the term implies – email is scanned for viruses in real time as it's being downloaded into your email program. If a virus is detected, that specific email is marked or disposed of in some way.

It sounds idea – with it turned on, presumably you can trust that if something actually was allowed to make it into your inbox by the scanner, it's likely to be malware-free.

Ideally.

Unfortunately, I've seen too many cases of these scanners running amok.

Real Time Email Destruction

The most common scenario I hear about sounds like this: "all my email is being deleted as it's downloaded".

That's almost certainly a real-time email malware scanner gone berserk. For whatever reason it's decided that every piece of email you're getting contains malware or is spam. As a result it's dutifully deleting them.

Every piece of email you're getting.

This is easily confirmed by turning that “feature” off in your anti-malware or anti-spam tool, and suddenly subsequent email resumes normal delivery.

Real time scanners have been implicated in more random email loss, email display issues as well as email program crashes.

As I said, I appreciate the concept, but the failures are still too common and the nature of the failures too severe for me to feel comfortable with them. Turning the feature off still corrects too many problems.

The Alternatives: Common Sense and On-Demand scanning

One of the most important skills you can develop as an internet user is the ability to detect suspicious emails. You know the drill: bad grammar, asking for private information and passwords, selling you suspicious merchandise or posing improbable scenarios. Those are all things you should be able to identify yourself without the need of some add-on tool.

And then there are attachments.

Naturally it's very easy to say "don't open attachments that you don't expect, or that you aren't 100% certain of".

On the other hand, to paraphrase a friend, if you get an email promising you that the attachment has dancing bunnies, you're probably going to do whatever it asks just so you can see the dancing bunnies.

Fine.

Scan the attachment first. Save it to disk, and then run your anti-malware tool(s) on the contents of the folder you saved it to.

If you like, exit your email program and instruct your anti-malware tools to scan all of your mail.

That on-demand scan doesn't interfere with your email program if the email program's not running. It's not going to prevent mail from being delivered because it's already been delivered.

It's simply going to scan the files already on your disk.

And presumably warn you if those bunnies will bite.

My Recommendation

My bottom line recommendation is this:

- Turn off real-time email scanning in your anti-malware tools
- Learn to spot and avoid malicious emails, even if - heck, especially if - that means you'll miss out on some dancing bunnies

- Run on-demand scans for anything you think might be suspicious, but that you can't resist opening
- Run a daily full scan of your machine for anything that might slip through. I do this at night when I'm not using the machine.

And if you do leave your real-time mail scanner enabled because you've never had a problem - you might at least suspect it if suddenly email starts getting deleted out from underneath you.

Related Articles on Ask Leo!

- The best anti-spyware, anti-virus ... and dancing bunnies? The best operating system in the world can't save you from dancing bunnies.
- What Security Software do you Recommend? - I have recommendations for specific products in various places on the site. Here's a short single page summary.

Article C4715 – January 20, 2011

Kill Spyware

Spyware is similar to viruses 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?

> Spyware and other forms of malware are only becoming more common. We'll review the steps you need to take to avoid spyware and its fallout.

Spyware is a modern scourge. It's certainly on the top 5 list of topics I deal with on a daily basis.

Some forms actually live up to the name and spy on you by monitoring and recording what you do. Others are worse: acting almost like viruses, hijacking your web browser, popping up ads, or just generally wreaking havoc.

Like viruses, spyware isn't going away any time soon. It requires vigilance on your part to avoid spyware.

There are three important steps to avoiding spyware:

-

1. Install and Run an Anti-Spyware Program

There are many options. These are the three most common free recommendations:

- I recommend Microsoft Security Essentials. A download from Microsoft, MSE acts as both anti-spyware and anti-virus. Microsoft Security Essentials replaces my previous anti-spyware recommendation, Microsoft Defender.
- Spybot Search and Destroy – Spybot does a great job of finding 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.
- Lavasoft's Adaware - Adaware is the other most commonly recommended anti-spyware tool. Adaware Free is available for personal home use.

Download and install the package of your choice.

Now.

Before you forget. 

2. Update the Spyware Database

New spyware is being created every day. As a result, the databases used by anti-spyware programs are being updated as well. You need to make sure that you always have the most current database.

After you install your anti-spyware tool, you should first update the database of spyware definitions that came with the installation. Many tools will actually do this automatically on setup, but you should make sure that it happens one way or another.

All of the programs listed above, as well as almost any other, will have automatic update features. The program will periodically locate, download, and install the latest databases automatically without you needing to do anything.

Make sure that that feature is enabled.

3. Run Regular Scans

Some anti-spyware programs now default to working automatically. Once Microsoft Security Essentials is installed, it goes to work protecting you right away, and defaults to performing a complete scan daily.

Others, however do not.

Regardless of which solution you choose - even if it's MSE - it's important to double check and enable automatic scheduled scans.

An Additional Recommendation

MalwareBytes Anti Malware tends to defy classification. It's not an anti-virus tool; in fact, the folks at MalwareBytes will recommend that you install a separate anti-virus tool along with it. Strictly speaking, it's not really anti-Spyware either, but that's definitely the closest classification if you insist on one.

Its name is appropriate - anti-malware - because it scans for and removes a wide variety of malware, often before other tools can do so.

It's a good tool to have on hand and run periodically or when you run into trouble. Like all such tools, it requires periodic database updates. There's a free version, which can only be run manually. The low-cost upgrade adds the ability to schedule scans.

Some Additional Notes

Many anti-spyware programs support advanced forms of real-time protection that can prevent spyware from installing. For example, they may lock your browser home page so that it can’t be changed without

your approval, or the "hosts" file may be altered, locked or removed. These techniques are very valuable, and I recommend turning them on.

As with anti-virus tools, there remains no single "best" anti-spyware program. Each 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.

Related Articles on Ask Leo!

- What Security Software do you recommend? I have recommendations for specific products in various places on the site. Here's a short single page summary.
- So just how sneaky can spyware be? Much of what we call spyware, like adware, can be relatively benign. But there's definitely the more intrusive, damaging kind of spyware as well.
- My anti-spyware tool is reporting errors in my hosts file. What is that, and why? The hosts file can be used to send you to or prevent you from reaching malicious sites. Different anti-spyware tools can bump into each other checking on this.
- Is running two anti-spyware programs better than one?
- With Microsoft providing Microsoft Security Essentials do I no longer need to purchase malware protection? Microsoft Security Essentials provides basic anti-virus and anti-spyware scanning for free. It appears to be a reasonable anti-malware tool for many.
- Viruses: How do I keep myself safe from Viruses? Computer viruses are a fact of modern connected life. Anti-virus software is required, and both it and the database it uses should be kept up-to-date.
- Do I need a firewall, and if so, what kind? Firewalls are a critical component of keeping your machine safe on the internet. There are two basic types, but which is right for you?

Article C2278 – June 10, 2011

So just how sneaky can spyware be?

> Much of what we call spyware, like adware, can be relatively benign. But more and more there's a more intrusive, damaging kind of spyware as well, better called "malware".

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

Spyware can be extremely invasive and, for lack of a better term, "sneaky".

There are some very frightening scenarios.

•

Much of what we've called "spyware" has for many years been relatively benign. It's been annoying and intrusive, but not particularly malicious.

However, particularly with the lines blurring between spyware and viruses, the fact is that most malware these days is far from benign. Not only can spyware "spy", it can push ads, infect other machines, send spam, and even in some scary scenarios poke around in your bank account when you're not looking.

The term "malware" - for MALicious softWARE - is actually much more appropriate these days as spyware is doing a lot more than just spying.

Let's look at the scenario you've outlined as an example. If your machine or your friend's machine has spyware of some sort it is very possible that it 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...

This is also a good example of the fact that there are both "good" and "bad" types of spyware.

While monitoring your IM conversations seems like a very bad thing on the surface, it's exactly what we ask parental monitoring and control software to do. Legitimate spyware that is, indeed, spying on you. These are commercially available packages that can be used by parents to monitor or control their children's internet use. Is it spyware? Absolutely, it is - it's spying on you. It could be used to do exactly the types of things we're talking about here, on purpose, and it would be a very legitimate use of the technology.

It could also be used by others to do exactly the types of things we're talking about here, also on purpose, but it would be far from a legitimate use - true "spying" in a very malicious sense.

And of course there are other, less legitimate instances of spyware that do the same or worse and really earn the moniker "malware". Perhaps one of the worst I've heard of recently is malware that inserts itself into your system and waits for you to connect to your bank to perform online banking. While you're connected it operates in the background and starts transferring money out of your account, which you don't see while it's happening.

Yes, spyware can be sneaky ... very sneaky.

That's why most tech support folks like myself seem to be constantly harping on anti-malware tools and general education about malware prevention.

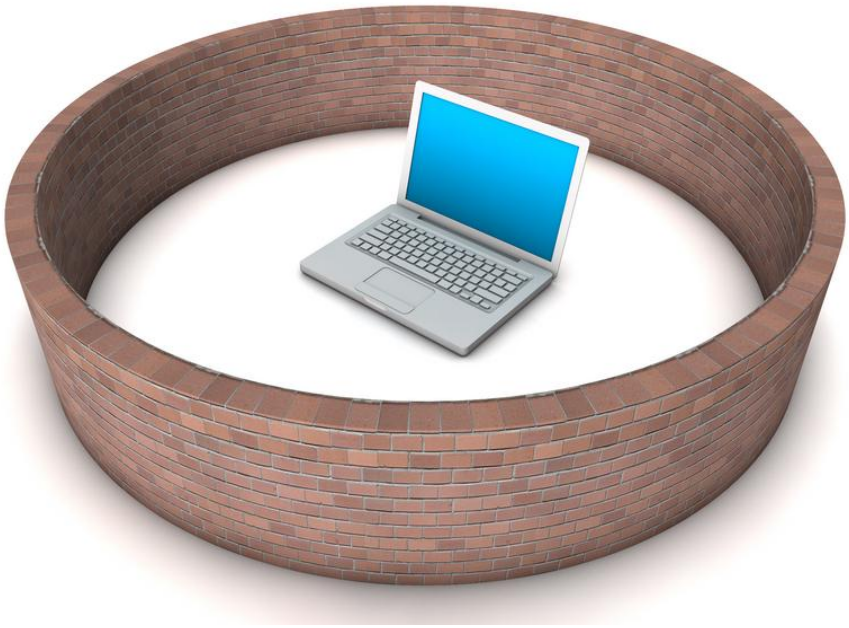
It really is that important.

Related Articles on Ask Leo!

- Spyware: How do I remove and avoid spyware? Spyware and other forms of malware are only becoming more common. We'll review the steps you need to take to avoid spyware and its fallout.
- What Security Software do you Recommend? I have recommendations for specific products in various places on the site. Here's a short single page summary.

Article C1990 - March 19, 2010

Use a Firewall



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?

A firewall is critical to keeping your internet-connected computer safe. We'll review what a firewall is and the two different types of firewalls.

I keep hearing the term "firewall" and how I need one when I connect my computer to the internet. What's a firewall, why do I need one and how do I set one up?

•

Many types of viruses and other types of malware can be prevented simply by using a good firewall.

In your car, a firewall is the "wall" of metal between you and the engine. Its purpose is to prevent engine fires from reaching you.

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

Let's look at the two common types of firewall.

•

Network-based threats

A firewall fundamentally protects your computer from network-based threats.

Almost all computers on the internet are under constant attack. Malware on other machines, hackers, bot-nets, and more are waging a slow but extremely persistent war, checking for any unprotected vulnerabilities on other internet-connected computers. If they find such a vulnerability, they then infect the machine that they've found or worse.

The basic concept of a firewall is very simple: it blocks or filters certain types of network traffic from ever reaching your computer.

Traffic that you want to reach your computer:

- Websites pages that you visit
- Software that you download
- Music or videos that you might watch
- And more...

Other traffic that you definitely don't want:

- Your neighbor's machine infected with a botnet trying to connect to your machine over the network to spread the infection.
- Overseas hackers trying to gain entry to your machine over the network to steal your personal information.
- And more ...

A firewall knows the difference.

Hardware firewalls, like your router

A router sitting between your computer and the internet is one of the most effective and cost-effective firewalls that the average computer use can have.

The router's job is to "route" data between the computers on your local area network and the internet.

Routers also allow you to share an internet connection by what's called "Network Address Translation". As it's more commonly referred to, NAT "translates" between your internet-facing IP address and the local IP addresses that have been assigned to your local machines by the router.

Routers then watch for connections initiated by your computer to resources out on the internet. When a connection is made, the router keeps track so that when a response comes back on that connection, it knows which of your local machines to send the data to.

The side effect is that if an outside computer tries to start a connection, the router doesn't know which computer to send it to. All it can do is ignore the attempt.

That effectively blocks everything on the internet from trying to start a connection to a machine on your local network.

And that makes your router a powerful incoming firewall.

Your router will not, however, filter outgoing traffic.

Software firewalls

Software firewalls are programs that you install on your computer. They operate at a very low level - as close to the network interface as possible - and monitor all your network traffic. While all of the network traffic still technically reaches your machine, the firewall prevents malicious traffic from getting any further. Much like a router, a software firewall prevents the rest of your system from even realizing that there is any malicious traffic.

In addition, some software firewalls can often be configured to monitor outgoing traffic. If your machine becomes infected and some malware

attempts to "phone home" by connecting to a known malicious site or tries to infect other machines on your network, a software firewall can often warn you and block the attempt.

All versions of Windows after XP have a software firewall built in and all versions after Windows XP SP2 have it turned on by default. Windows may even annoy you into ensuring that the firewall is either turned on or that you're aware of the risks in not having it turned on.

The Windows firewall is primarily an incoming-only firewall.

Choosing and setting up a firewall

In general, I recommend using a broadband router as your firewall.

There is disagreement as some believe that an outgoing firewall is important. My position is that an outgoing firewall doesn't really protect, but it simply notifies after something bad has happened.

Routers are pretty common and nearly a requirement for anyone who has more than one computer sharing an internet connection. If you have a NAT router, you have a firewall without needing to burden each computer with additional software.

Software firewalls do make sense in a very important situation:

- Software firewalls are critical when you can't trust other computers on your local network.

Don't trust the kids' ability to keep their computer safe from? Enable the software firewall on your computer.

Heading out to the local open WiFi hotspot? Turn on the Windows firewall immediately.

In later versions of Windows, the built-in firewall has matured to the point where it's actually quite reasonable to leave it on all the time, even if you're behind a router. It seems to impact operations very little and saves you from remembering to turn it on when you travel or have that not-so-trustworthy guest on your network.

Firewalls are only a part of the solution

The bad news is that a firewall can't protect you from everything. A firewall is focused on protecting you from threats that arrive via malicious connection attempts over the network. A firewall will not protect you from things that you invite onto your machine yourself, such as email, attachments, downloads, and removable hard drives.

Nonetheless, protecting from network remains critically important.

Related Articles on Ask Leo!

- Firewalls Using a firewall is an important first line of defense against network-borne threats to your computer. This section covers questions and answers relating to both hardware and software firewalls, why you need one and when you might not.
- What are these access attempts in my router log? Any device sitting on the internet is subject to a constant stream of "internet background noise". It's why you really want to be behind a firewall.
- Do I need a firewall, and if so, what kind? Firewalls are a critical component of keeping your machine safe on the internet. There are two basic types, but which is right for you?
- How do I turn off the Windows firewall warning? If the Windows firewall is not enabled, Windows will warn you. You can tell Windows that you know what you're doing and don't need the Windows firewall.
- Windows Firewall is restricting access to something I want ... what do I do? If Windows Firewall is restricting access to a program you want, there are a few steps to take to allow them access to the internet once more.

Article C1941 – June 5, 2011

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

> Firewalls are a critical component of keeping your machine safe on the internet. There are two basic types, but which is right for you?

I keep hearing about "firewalls" for my computer and that there are different types. Do I need one? If I do, what kind of firewall do I need?

•

The very short, very easy answer is: hell yes! Absolutely, positively you need a firewall.

With all that happens on the internet these days it's simply too risky to let your computer sit "naked" on the internet unless you really know what you're doing.

The real question is then: what do you need?

Heck, it's even possible you already are behind a firewall and don't need anything more.

•

Realize that a firewall is about protecting you and your computer from them where "them" means "the malicious folk on the internet".

A correctly configured incoming firewall does not block your access out to the internet. You should be able to browse the web, for example, without interruption. The firewall prevents access from somewhere on the internet to your computer. That's not to say people can't send you email; they can because you access your mail through the internet by going out to get it when you download it. It does mean that people can't copy files directly to your PC or cause programs to be run on your machine remotely.

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.

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 firewall - an additional device you place between your computer and your internet connection - or a software-based firewall - a program that you install on your PC?

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 act as firewalls providing an exceptionally high level of protection quite literally right 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. You can read more about routers and how I'd set up a home network. Remember, a router will work just fine even if you have only one computer.

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, Vista and 7 all include one by default. Even if you do nothing else and you're not sure what you really want to do, you should simply make sure that the Windows Firewall is turned on. Check in the "Security Center" in Control Panel.

There are many other popular firewall packages, though I typically recommend against all-in-one "Internet Security Suites" as provided by many manufacturers. Instead, a dedicated firewall such as Comodo or others might be well worth investigating.

One of the biggest differences with software firewalls, particularly third party offerings is the ability to provide outbound protection. As I said above, a firewall's primary job is to protect your computer from internet based threats. However, if you've been compromised an outbound firewall will often prevent the attack from spreading from your computer to others, and will alert you when something suspicious has happened. While I don't typically view an outbound firewall as absolutely necessary, it's another part of the puzzle that's at least worth considering.

Finally, when you believe you're protected or even if you know you're not visit Gibson Research and run "Shields Up", a vulnerability analysis. It will try to access and analyze your computer from the internet and will list for you exactly how you are vulnerable. It tends to be a tad alarmist in its wording, and getting a perfect score is almost impossible, but it's valuable information to help you decide if you need to take additional steps.

Related Articles on Ask Leo!

- What's a firewall, and how do I set one up? A firewall is critical to keeping your internet connected computer safe. We'll review what a firewall is and the two different types of firewalls.
- Is an outbound firewall needed? Many software firewalls will alert you on suspicious outbound connections. The biggest problem is that if correct, by then it's too late.

Article C1911 - December 26, 2009

Does my router have a firewall or not?

> Most routers both do, and do not, have a firewall. The good news is that the protection offered by a router's firewall is often exactly what you need.

I purchased and installed a broadband router. Specifically, a wireless Linksys WRT54G. I thought this provided a firewall and I had planned to uninstall Norton Systemworks which is giving me problems. However, the router does not appear to include a firewall. It does not need any sort of configuration like Norton, such as sites to let through or to block. I have looked all through the documentation and no mention of a firewall.

Did I buy a model without a firewall or was I mistaken about a router including a firewall?

•

Your router does, and does not have a firewall.

And I totally understand that this is confusing.

I'll try to clear it up...

•

One of the things that your router does is allow you to share your internet connection. By that I mean you can take a single internet connection that's designed to connect to only one computer, add a router, and then through the router connect several computers who can then use that single internet connection.

The way this happens is that your internet IP address, which is used to route data to you when you surf the internet, is assigned to the router instead of a computer. The router then assigns local IP addresses to each of the computers you have connected to it. The router then also takes care of making sure that the data sent to and from the internet is routed to and from the correct computer on the local network.

One side effect of this approach, called Network Address Translation, or NAT for short, is simply this: no computer from outside your local network can initiate a connection to a computer on the inside of your local network.

Put another way: computers on the internet are completely blocked from connecting to computers behind a router. (You can create exceptions, of

course, using something called "port forwarding" and/or "DMZ" settings in the router configuration.)

In this regard, the router is acting like an inbound firewall. In fact, it's acting so much like one that we simply refer to it as being a firewall.

Now, in the strictest sense, your router is not truly a firewall. Two key components are missing:

- Your router does not attempt to block any outgoing connections or data. A true firewall will typically examine outbound connections as well as incoming. In fact, a great deal of the configuration you referred to in your question is typically defining to a firewall exactly who on your computer is allowed to make an outbound connection.
- Your router does not inspect the data that's routing, other than to make sure it's headed to the correct computer. Firewalls are often configurable to the extent that you can allow not just certain types of connections, but also allow, or block, certain types of data over those connections. In the extreme a firewall could actually incorporate anti-virus checking and block anything that was found to be carrying a virus.

So in that regard your router is not a true firewall.

So what do you need?

In my opinion: if you can trust all the computers on your local network, a NAT router provides 99.9999% of what you actually need in a firewall. Blocking external threats is by far the single most important role of a firewall these days; so much so that everyone should have some kind of firewall, no matter what.

In my opinion a software firewall is simply not needed in this case. Blocking outgoing traffic sounds important, but in reality, if you have outgoing traffic that needs to be blocked, then either you need to change your system's configuration not to try to do whatever it's doing, or you are already infected with malware. In the later case, it's too late. The firewall did not prevent you from getting infected. At best it might have prevented you from infecting someone else, but even that is suspect.

Now, you'll notice I emphasized the phrase if you can trust all the computers on your local network. That's the one exception to the "software firewalls not needed" guideline. For example let's say you share your computer connection with your children who don't understand internet safety and are constantly getting their computer infected. In a case such as this, where you cannot trust some other machine that shares your local network with you, then you probably do need a firewall to protect you. And let's be clear; that firewall is not to protect you from the internet -- your router does that -- but from that other machine. And once

again, what really matters here is blocking unwarranted incoming connections. As far as I'm concerned if the firewall lets you disable monitoring of outgoing connections, you can.

So if you're in that "safe" situation, then yes, in your shoes I would uninstall that software firewall and rely on the protection of my NAT router.

In fact, that's exactly what I do here at home.

Related Articles on Ask Leo!

- What's a firewall, and how do I set one up?
- Do I need a firewall, and if so, what kind?
- Recommendation: Firewalls

Article C3323 - March 17, 2008

Is an outbound firewall needed?

> Many software firewalls will alert you on suspicious outbound connections. The biggest problem is that if correct, by then it's too late.

Isn't an outbound firewall really important in many situations? I deliberately installed a free version of a key logger on my system and ran thorough scans through my anti virus and anti spyware programs. But the running key logger wasn't detected even though the key logger icon was right there in the system tray.

You have said that when an outbound firewall stops something it is already too late. But don't you think outbound firewall might stop a key logger from at least sending logs to an email or remote computer? Or would it not?

•

A firewall with outbound detection can have a place, I suppose, but you've captured my thoughts already: if it finds something to detect, then it's too late.

Let's review what it means to be an outbound firewall, why I don't value them all that much, and perhaps why your key logger wasn't detected.

•

Firewalls protect you from the certain classes of bad things out on the internet.

Note that's "protect you from them". That implies that the primary function of a firewall is to prevent bad stuff "out there" from reaching or affecting your computer.

My preference is to use a hardware device such as a router with NAT (Network Address Translation) enabled. This does an incredibly effective job of hiding your computer from outside access. You can connect out, but outside computers cannot initiate a connection without your having explicitly configured your router to allow it.

Using a router also takes the burden of that work off of your computer. In fact, a single router can act as a single effective inbound firewall for all the computers that are connected behind it.

An "outbound" firewall looks for threats originating on your computer attempting to connect out to the internet. In a sense, it's "protecting them from you". While that may be very generous of you to protect everyone else from your computer, the real difference is that it will presumably

block and more importantly tell you when something suspicious is happening so that you can take corrective action.

Outbound firewalls have several shortcomings, both technical and conceptual:

- It's too late. As you pointed out, if an outbound firewall detects something that is, in fact, malicious in nature it's because your machine is already infected. Something in your inbound defense failed and your machine has acquired some form of malware. Yes, I suppose it'd be nice to know, but in fact those very inbound defenses - firewall and anti-malware scanners - should have already either prevented or detected the problem. With adequate inbound protection, an outbound firewall is redundant.
- It's intrusive. Outbound firewalls are only practically available as components of software firewalls that you install on your machine. As such, these firewalls take up additional resources to do their job. Rather than do that, a router will give you the inbound protection you need without taking up additional resources on your machine.
- It's frequently wrong. One of the very common complaints about outbound firewalls are warning messages that are either incomprehensible, overly frequent, or don't give the average user enough information to make an informed decision. Frequently, they'll simply report a connection attempt to or from an IP address with little or no additional information. I also commonly see people asking about warnings that arise from totally legitimate processes on their machine accessing the internet for things like software updates or the current time and date. With too many errors, indecipherable messages or false positives, people tend to ignore the warnings after a while, rendering the outbound firewall ineffective.

Now, don't get me wrong: software firewalls do have their place. In particular, when traveling and using open WiFi hotspots I'll absolutely turn on the built-in Windows firewall. Software firewalls are also a good choice if you have no router, or if you cannot trust the other computers that share your router. But in either case that's for the firewall's incoming protection against external threats, not the outgoing.

Is there a case for an outgoing firewall at all? Many experts will disagree with me and say absolutely, that they add a lot of value and that the issues I've raised are simply off target or over-stated. But I remain of the opinion that if an outgoing firewall is, in fact, adding value it's because your incoming protection is inadequate. If you're going to focus additional energy and resources at becoming more secure, I'd much rather have you

focus on preventative solutions rather than solutions which will only kick in after it's too late.

Now, about your key logger.

My first reaction is that if it's showing up in the system tray I'm not sure I'd classify it as malware. It's open about what it's doing, and easily visible. A key logger isn't in and of itself necessarily malware - there are many legitimate uses for the technology. So part of my reaction is that I'm not really surprised that it wasn't detected as malware, because it's not behaving like malware.

But lets assume that you did get infected by a truly malicious key logger - one that was attempting to hide, and send all your keystrokes to some overseas hacker. Well, at the risk of repeating myself too many times: it's too late. Your machine has been compromised, and you can no longer trust it; and that includes trusting your firewall. Yes, your outbound firewall might block the transmission - or it might not. The malware could, in fact, include additional code to actually reconfigure your firewall to let the malware's communication through. It's been done.

This is almost worse than having no outbound protection at all. With the outbound firewall you might think you're protected, but in fact you're not. Without an outbound firewall, you know, and you know to focus your efforts on inbound protection to avoid the problem in the first place.

Like I said, I know that others will disagree with me, and I'm sure there'll be some compelling cases made in the comments.

But I'm not convinced, and outbound firewalls are not something I use or advise.

Related Articles on Ask Leo!

- What's a firewall, and how do I set one up? Firewalls are an important part of keeping your computer safe when connected to the internet. We'll look at what a firewall is and your choices.
- Can a computer virus spread behind my firewall? Computer viruses spread in different ways. A firewall is very important but some computer viruses can spread on your local network if they make it across.

Article C3484 - August 29, 2008

So do I need the Windows Firewall or not?

> You do need a firewall and particularly if you aren't behind a router the Windows Firewall is one option.

I'm really confused. With the new Windows XP SP2 Security Alert System, do we still need a firewall to stop outbound traffic? If we get a router, (LINKSYS), does that take care of everything, which means we need to disable Windows Firewall to avoid false alarms?

•

There's a lot of misunderstanding about firewalls, routers, and other security software. When Windows XP service pack two was released it definitely put security and particularly the firewall, "in your face". Subsequent releases of Windows now also include the firewall and turn it on by default.

It's a great opportunity to find out what you need ... and what you don't need.

•

A firewall filters network traffic. A previous article "What's a firewall, and how do I set one up?" covers this in more detail, but the bottom line is that a firewall primarily protects you from certain classes of incoming network-based problems.

Every computer should be behind a firewall of some sort.

In general, hardware firewalls, typically provided by NAT routers, keep malicious network 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 network address translation, or NAT, enabled (most consumer grade routers do, by default) 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 at least want to turn on the Windows firewall. This is what I do when I take my laptop with me on the road - not being sure of exactly what I'm connecting to, the firewall protects me from network based threats.

Now, one word in the original question is worth a comment: "outbound".

Consumer grade routers will keep you safe from threats that are incoming from the network, but will not filter or warn you of any malware already on your machine attempting to connect out. The Windows firewall has a limited amount of outbound traffic alerts, and other software firewalls that you can install separately to use instead of the Windows Firewall can be configured with a wide array of outgoing protection.

There's a wide variety of opinion on this, but personally, I'm quite happy simply behind a router and with no outgoing threat monitoring.

But regardless, you do need a firewall; be it an external router, a software package that you install, or at a minimum simply enabling the Windows Firewall already present on your machine.

Related Articles on Ask Leo!

- What's a firewall, and how do I set one up? A firewall is critical to keeping your internet connected computer safe. We'll review what a firewall is and the two different types of firewalls.
- How do I turn off the Windows firewall warning? If the Windows firewall is not enabled, Windows will warn you. You can tell Windows that you know what you're doing and don't need the Windows firewall.
- Is an outbound firewall needed? Many software firewalls will alert you on suspicious outbound connections. The biggest problem is that if correct, by then it's too late.

Article C2186 - February 21, 2010

How do I change my router's password?

> Changing your router's password is important, but the steps aren't always obvious. I'll walk through changing my router's password.

How does one change the router password? Where are the controls and settings for the router?

•

I recently wrote about several steps you should take to secure your router. One of those steps is to change the default password.

Several people wrote in to ask how to do that, as it's not at all clear how you access your router settings at all, much less the password screen.

I'll show you, step by step, how I access the settings on my LinkSys router.

•

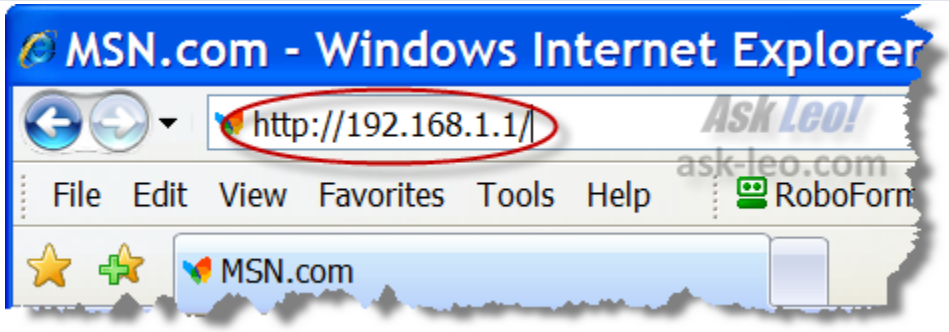
Now, I have to start by saying that unless you have a LinkSys, perhaps even the exact same model, your steps may be somewhat different. You really should be checking the documentation that comes with your router to get the specifics necessary to change settings on your device.

That being said, the concepts are generally the same for most consumer routers, and hopefully this will help you interpret those instructions a little more easily.

We start with your browser.

Routers don't have applications or settings that you'll find on your computer anywhere. They're a separate device on your network, and as such need to be accessed across the network. Most router manufacturers have made this fairly easy by including a mini web-server inside the box that you use to access the settings.

You access your router's settings by entering its IP address in the address bar of your browser:



192.168.1.1 is a pretty common IP address for routers on small networks, but if that's not it, another "trick" that occasionally works is to open up a command prompt, enter "ipconfig" (followed by Enter), and look for a "default gateway":

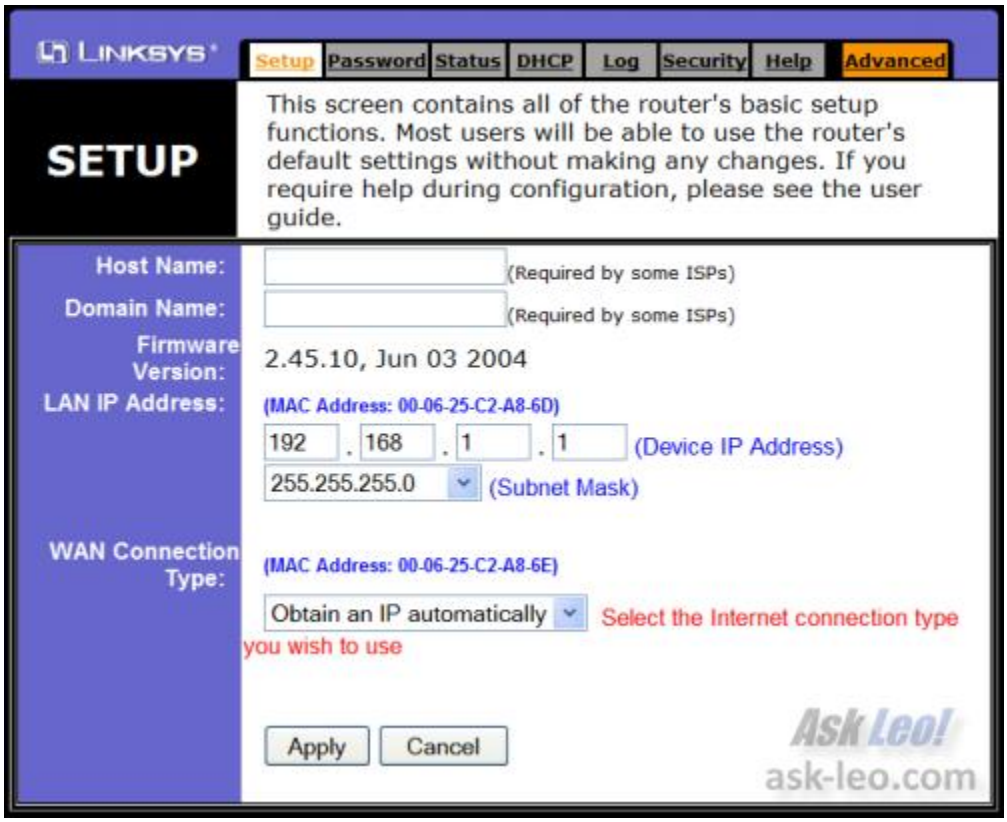
```
Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . :
IP Address. . . . . . . . . . . . : 192.168.1.5
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
```

In most cases, that's the IP address of your router.

Once you've entered your router's IP address into your browser's address bar and pressed "Enter", you should get an authorization request:

Most all manufacturers have default settings for this. For example, if you have a LinkSys, the default is to leave the User name blank, and enter "admin" as the password. It's this very default setting that we're going to change, because as you can see - everyone knows it.

Once you enter the correct user name and password, press OK and you should land on your routers "home page" for configuration.



As you can see there's a "Password" tab at the top of this UI. Clicking it takes you to the Password management page.

In typical password-setting practice, you enter your new password twice, and press Apply.

Your router has a new password.

A couple of additional notes on your new password:

- Do Not Forget It - keep it somewhere safe. If you forget your password you'll be unable to access your routers settings. On most routers that means you'll need to perform a "reset to factory defaults", which will reset the password to its default, as well as erase any and all other settings you may have changed.
- Choose An Appropriate Password - access to your router can be used for many things besides just playing with a few settings. Malware has been known to perform complex spoofing attacks simply by altering how and where the router gets its DNS information, for example. You'll want a strong password to protect it. Since this is a password you enter infrequently, it's worth it to make sure it's secure even if it is difficult to enter. I recommend using, say, the first 10 or 12 characters of a random password created by a good password generator.

As I said at the beginning, unless you have the same exact router that I do, it's likely that the details of what I've shown will be different for you. Check your router's documentation for the exact steps to perform this change.

But do change your router's password. The default password is about as secure as having no password at all.

Related Articles on Ask Leo!

- How do I secure my router? Your router is your first line defense against malicious attacks from the internet. But is your router secure? I'll review the important settings.
- Change Your Password - No, not that one... You probably need to change a password, but not the one you think.
- Does sharing a router make me vulnerable to those I share with? Being on the same local network as another machine implies a certain level of trust. Without that trust, additional security steps are called for.

Article C3674 - March 13, 2009

How do I secure my router?

> Your router is your first line defense against malicious attacks from the internet. But is your router secure? I'll review the important settings.

I'd like to know how to clear the history of my Linksys Cisco router. I'd also like to know how I can protect it from hacking and who else besides the people that know my router's WPA code can view browsing history.

•

There are a couple of misconceptions in your question, which I'll clear up in a second.

The more general topic is an important one: how do you make sure that your router is secure? After all, as your firewall it is your first line of defense against malware trying to get at your computer from the internet.

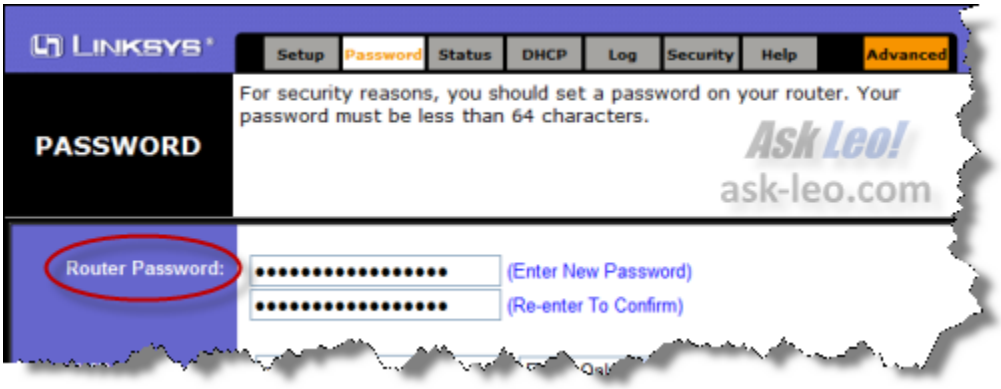
•

First, most routers don't maintain a history, so there's nothing to erase, and nothing for anyone to view. Most routers just ... route. However there are sometimes ways to enable a certain amount of logging, and we'll look at that below.

While the concepts below apply to almost all consumer grade routers, I'll be using my own Linksys BEFSR81 Router, and Linksys WAP54G as examples. You'll need to "translate" the examples to the equivalent settings on your own router or access point.

Change The Default Password

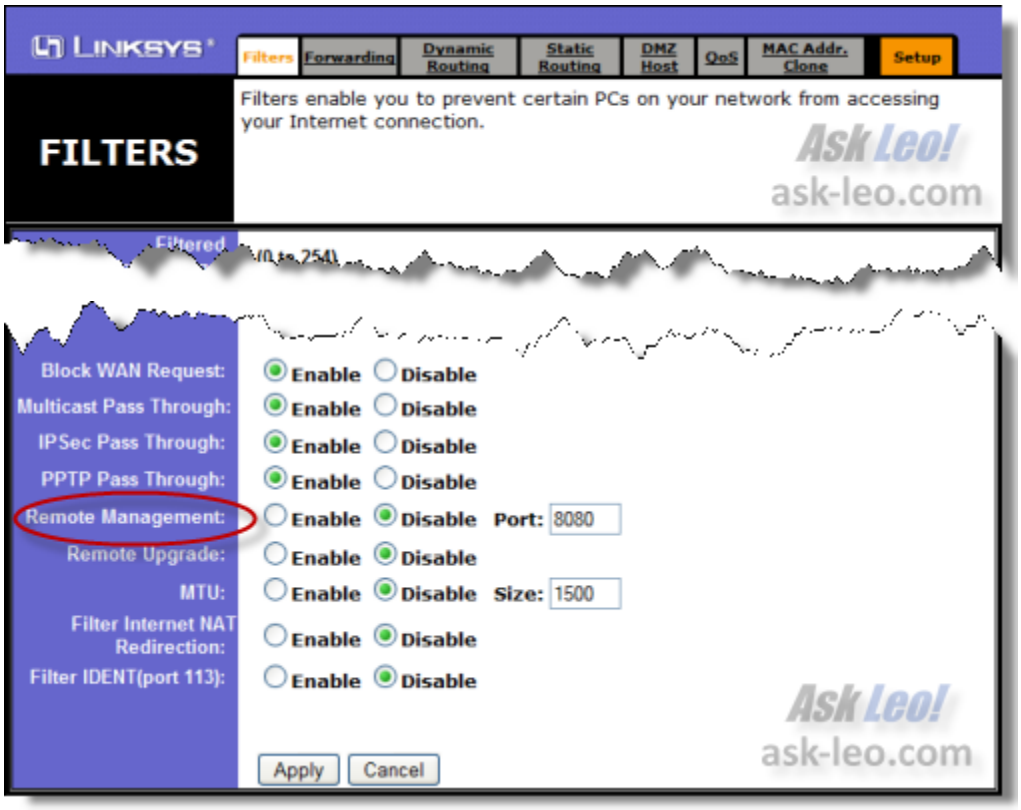
If you do nothing else to your router, change the default password now. Change it to be something strong - obscure passwords like "I2tX3ZPz2hMszg" are perfect. (If you don't have a random password generator, GRC's Ultra High Security Password Generator is a great tool.)



The reason for this is simple: every router and access point is shipped with the same default password. For Linksys, if your login is a blank username and a password of "admin", everyone knows it. And anyone can then login to your router and undo any and all of the security steps we're about to take. (There is also malware that takes advantage of the default passwords on routers to make changes without your knowledge.)

Disable Remote Management

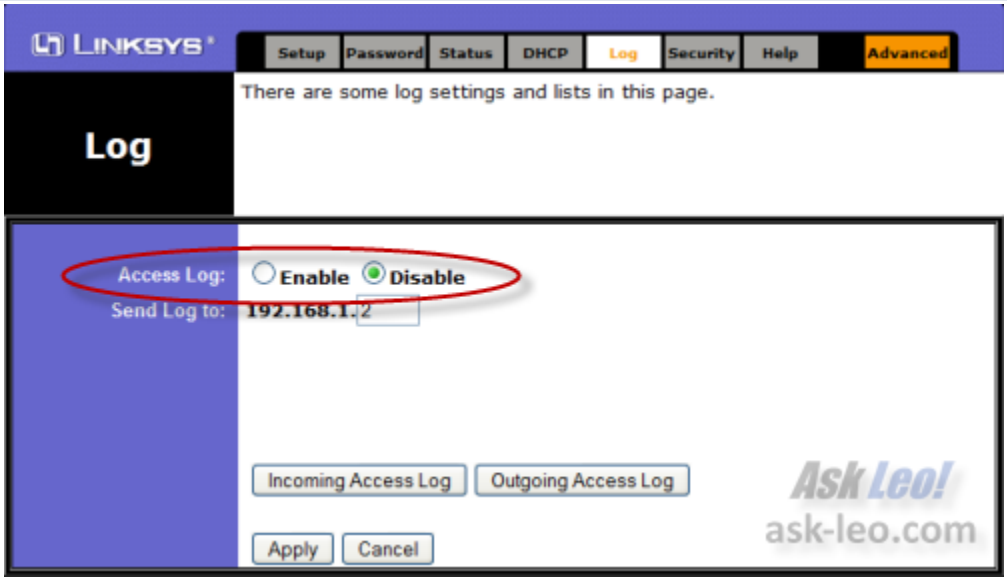
"Remote Management" is a feature whereby your router can be administered remotely - in other words from anywhere out on the internet.



While this setting (coupled with a very strong password) might make sense for a handful of people, for most folks there's absolutely no need to administer the router from anywhere but your local machines connected to it. Make sure that remote management setting is off.

Turn Off Logging

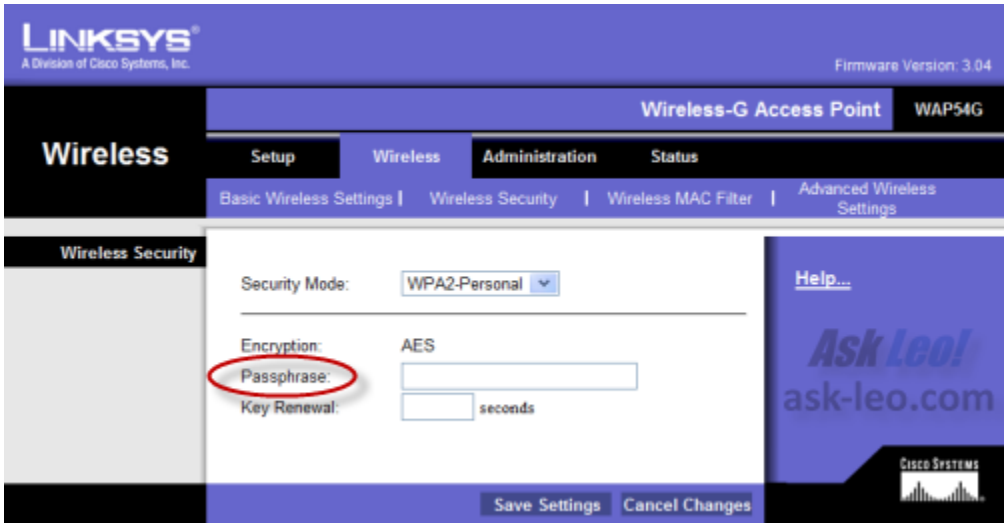
OK, more correctly, this is "make sure logging is still turned off", since if a router supports any kind of logging at all, it'll likely be off by default.



Disable the logging, and no information will be kept on the router, or sent to any other machine.

Add a WPA Key

It's time for another password, this time to secure and encrypt your wireless connection.



First: use WPA, not WEP. WEP encryption turns out to be easily crackable.

Second, select a good, secure key/password/passphrase (the terms are roughly interchangeable here). A passphrase generated by the GRC Password Generator would be a good choice. You only need to enter it once here, and once on each machine that is allowed to connect to your wireless network.

Having a strong WPA key ensures that only machines you allow on your network can see your network, your traffic, and your router.

Don't Forget The Physical

All of your router settings can be reset in a flash if someone has physical access to the device. Almost all routers have a "reset to factory defaults" mechanism - typically by holding a reset button for a certain amount of time. If someone can walk up to your router and do that, then all the security settings you've just enabled may be instantly erased.

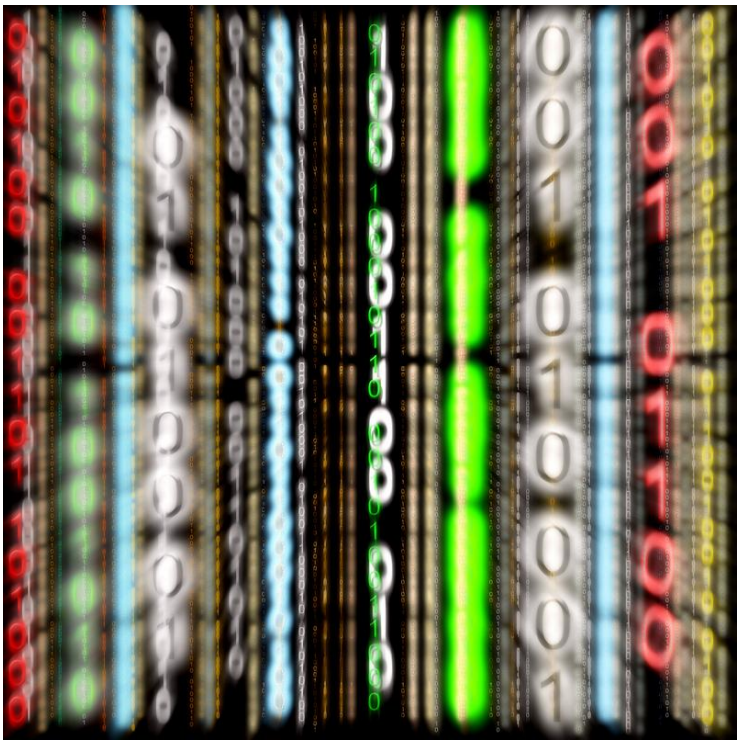
Only you can judge whether or not you need this extra level of physical security, but make sure to consider it.

Related Articles on Ask Leo!

- Change Your Password - No, not that one... You probably need to change a password, but not the one you think.
- What are these access attempts in my router log? Any device sitting on the internet is subject to a constant stream of "internet background noise". It's why you really want to be behind a firewall.
- Does sharing a router make me vulnerable to those I share with? Being on the same local network as another machine implies a certain level of trust. Without that trust, additional security steps are called for.

Article C3669 - March 8, 2009

Stay Up-To-Date



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 years ago. The solution is simple: enable automatic updates, and visit Windows Update periodically. And make sure that your security software and applications are also being updated regularly.

Are automatic updates a good thing?

> Unless you're willing to pay a lot of attention on a very regular basis, automatic updates are an important part of keeping your machine safe.

What are your thoughts on automatic updates? Not Windows updates but automatic updates for my spyware and antivirus programs. I have many anti-spyware and McAfee internet security suite and I have automatic updates turned on on all. Could this lead to problems by leaving my computer open to the net?

•

This one's easy: I love automatic updates.

Let me explain why, and some of the things to look for to make sure that your automatic updates are safe, and doing what you think.

•

First, I believe strongly that automatic updates for anti-spyware and particularly anti-virus packages is an absolute must. There are simply too many changes - quite literally every day - that keeping them up to date is a must. Doing it automatically is by far the easiest and most reliable way.

Application updates I treat differently. I still want automatic notification of updates and new versions, but:

- the update notification should be a true notification - not a regular "do you want to check for updates now" - check it for me, and bother me only if there is something I should be aware of.
- the update notification should tell me what it is, and what it's going to do for me - including how important or critical the update might be
- I should be able to choose not to install the updates right now, but rather be reminded later
- I should also be able to choose not to install the update at all, at least until the next, new, update becomes available.

There are some software packages that do all that, and I really do appreciate them.

And typically, I do accept the updates, but at a time that's convenient for me.

Windows update is a special case. I believe that most users should have automatic updates turned on, and automatically install all updates. That

being said, I have it set to notify only, and actually examine the updates being offered before I say yes. And I always say yes.

The relationship of Automatic updates to Windows update is another case of a missed opportunity as well. It appears that Automatic updates only deal with critical issues. If you actually visit the Windows Update site, you may find additional updates that you were not alerted to. (Like Office SP2, which I just now learned of as visited the Windows Update site.) I would prefer some kind of proactive notification for those as well.

As to your concern about security - in a nutshell, I'm not terribly concerned. Most automatic updates are handled through the same mechanisms that your web browser uses to visit web sites. The result is that for most, you're not "opening up" any additional vulnerabilities by enabling automatic updates. And as long as your dealing with reputable vendors, the chances of "automatically" downloading some kind of malware is next to zero. You're at much greater risk by mistakenly clicking on an emailed attachment, not being behind a firewall, or visiting a malicious web site.

Related Articles on Ask Leo!

- How do I make sure that Windows is up-to-date?
- What's this new 'Security Center' thing in XP service pack 2 all about?

Article C2491 - December 16, 2005

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

You can make sure that Windows is up-to-date by either enabling Automatic Updates or by visiting the Windows Update web site.

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 weekly. With that rapid a rate, how should you stay on top of things and make sure that your system is up to date?

There are several options.

•

Microsoft provides a service that runs on your machine and - on terms you control - automatically checks for Windows updates. Once found, it can then download and install them for you.

The specific labels vary slight across Windows versions, but to configure automatic update click on Windows Update in the Windows Control Panel.

In Windows 7, this is the Windows Update options dialog:

You have four basic options controlling how Automatic Update works:

- Never check for updates - as you might expect this basically turns the Automatic Update feature off.
- Check for updates but let me choose whether to download and install them - with this setting, Windows Update will only check the Microsoft 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.
- Download updates but let me choose whether to install them - with this approach, Windows Update will check the Microsoft site for updates and actually download any that apply. Once downloaded, you're notified that they're available and can initiate the install at your convenience.
- Install updates automatically - finally, you can just have Windows Update do it all, on a schedule you can define. Check, download, and install as soon as updates are available. (Note that depending on the updates you receive, your machine may be rebooted as part of this process.)

In Windows 7 you can also control whether or not the process should include both important and recommended updates, or just important. (You can still receive important and other updates by visiting the Windows Update web site, which I'll discuss below.)

Windows 7 also allows you to specify that all users can install system updates via Windows Update, and whether or not Windows Update should also update other Microsoft software on your machine (aka "Microsoft Update" as opposed to just "Windows Update").

For what it's worth, I like to know what's happening to my machine(s) before it happens so I typically select the "Download, but let me choose" 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 versions. That list is then compared against the latest releases and you'll informed of the differences. You can then select which components to install.

Related Articles on Ask Leo!

- Are automatic updates a good thing? Unless you're willing to pay a lot of attention on a very regular basis, automatic updates are an important part of keeping your machine safe.
- What's this new 'Security Center' thing in XP service pack 2 all about? Windows "Security Center" is an attempt to raise awareness about security issues while making it a bit easier to deal with.
- Internet Safety: How do I keep my computer safe on the internet? Internet Safety is difficult and yet critical. Here are the seven key steps to internet safety - steps to keep your computer safe on the internet.

Article C2024 - December 6, 2009

Get Educated

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.

What's a good password?

> Good passwords are hard to crack and hard to remember. As a result, many people don't use really good passwords, even though they should. We'll look at what makes a good password, and some ways to make them easier to remember.

I told my friend my password, and she said it was a really bad one. What does it mean to have a "bad" password? And what's a "good" one, then?

•

You told someone else your password? Yikes! I've seen more accounts get stolen by that one simple act than by any other single cause. I sure hope you know what you're doing - most people that have told a friend their password have come to regret it.

So what's a bad password? One that someone could easily guess.

A good password? One that's hard to guess, of course.

The problem is that people are way better guessers than you think. And it gets worse if the guesser starts using a computer to do the "guessing" for them.

•

What's a bad password?

A bad password is any password composed of common words or names, particularly if the password is short. For example, "iLoveMikey" is a bad password. "mydogspot" is a bad password. "GeorgeInParis" is a bad password. All are simply combinations of words or names. On top of that, many people choose bad passwords that express information that someone who knows you might be able to guess. If your boyfriend's name is "Mikey", your dog's name is "Spot", or you met someone named "George" during a trip to Paris, these are all things that people who know just a little about you can use to start making some educated guesses as to what your password might be.

And as I said, people can be really good guessers.

The irony is that the people who know you the best - your friends - are the ones who can probably make the best guesses and are the most likely to guess your password if it's a bad one.

Another problem with passwords made up from words and names is that it's really easy for a determined hacker to set up a computer with a

dictionary of words and names and have it start trying combinations until something works.

What's a good password?

A good password is a long random sequence of characters - letters, numbers and any "special characters". "qicITcl}" is a good password. "rAg2imWOIgIf47IM24busml6kpetPF9UGRpPAFBMCoSmSTptbDcOxwcG3a Poa79" is a great password. The best passwords are made up of completely random characters and as long as you can make it.

You can see the problem - great passwords are impossible to remember. So if you can't remember it, what good is it?

The solution is either a compromise, or the use of some technology.

The compromise

The compromise I use works like this:

- I never include full English words or names - instead I use misspellings or phonetic sound-alikes
- I always include a mix of uppercase and lowercase letters and numbers
- I always make sure the password is at least eight characters long, preferably longer

So, for example, while "Macintosh" is bad, "Mac7T0sh" might be good and probably easier to remember. "HondaPrelude" is bad, but "Pre7ood6" is much, much better.

The bottom line for this compromise: pick a random looking password that YOU can remember but that "they" would never guess - and as I've said a couple of times, always assume that "they" are always really great guessers.

Using Technology

Never, ever, write your password down on a piece of paper near your computer. Paper is definitely not the technology I'm talking about. It's amazing how many passwords are stored on sticky notes right on the monitor, under the mouse pad or in a desk drawer. It's not that hard for the motivated to go searching and find all that.

My old approach was to use an Excel spreadsheet with all account names and passwords - in fact I still do for much of my sensitive information. By itself, that's incredibly insecure and dangerous. Anyone who can get a hold of that spreadsheet has everything. Other people use simple text files

that suffer from the same fundamental flaw - it's the moral equivalent of a sticky note. Anyone who has access to the file has all the passwords.

The solution is to encrypt the file. I'm not talking about the encryption built into applications like Excel - which I'm led to believe is reasonably easy to defeat - but an "industrial strength" encryption solution such as TrueCrypt. Using TrueCrypt, you can control exactly when the information is actually visible, and the rest of the time it remains safely encrypted.

My current approach for website logins is to use RoboForm. RoboForm captures passwords when you enter them as you visit websites requiring login and then remembers them for you in an encrypted database. When you return to that site, RoboForm makes the login available for you automatically. It includes a handy random password generator. Since RoboForm remembers passwords for you, you can use completely random strings - the most secure passwords possible, as I described earlier.

But - be aware that RoboForm and the TrueCrypt-style of encrypted solutions both require one thing: a password to decrypt the database of passwords. That password needs to be something you can remember, yet something secure. However, remembering that one password then opens up the vault to your entire set of accounts and passwords.

Related Articles on Ask Leo!

- How do I keep from getting my account hacked?
- Dictionary Attack: What is it?
- How can I keep data on my laptop secure?
- RoboForm
- TrueCrypt
- Ultra High Security Password Generator

Article C2799 - October 1, 2006

How long should a password be?

> For years, the standard practice has been to assume that eight-character passwords made up of sufficiently random characters was enough. Not any more.

For a long time, the common thinking was that the best, most practical passwords consisted of a random combination of upper and lower-case letters, numbers, and a special character or two; if so composed, a password needed to be only eight characters in length.

Randomness remains important, but as it turns out, size matters more.

A password today should have a minimum of ten characters, and ideally, twelve.

•

Large scale account hacks

When you hear about large numbers of accounts being stolen by a hack at some service provider, you are naturally concerned that the hacker might now have access to your account names and passwords. If the service was storing your actual passwords, that could indeed be the case. (As I've said before, if a service is storing your actual passwords, then they simply don't understand security or they have made some horrifically bad decisions.)

In fact, most services will store an encrypted (technically, a "hashed") form of your password. For example, if my password were "password" (and that's a very poor password, of course), then a service might store "5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8" which is the hash value that corresponds to that password.1

What that means is that hackers do not get a list of user names and passwords. What they get is a list of usernames and password hashes.

And what's great about hashes is that you can calculate a hash from a password, but you cannot do the reverse - you cannot calculate the password from the hash.

---

1 For the technically curious, I'm using an un-salted sha256 as the hashing function here. That's technically better than md5 or sha1 that's commonly used.

As a result, one would think that by being hashed it'd be pretty unhackable, right?

Sadly, not so much.

Dictionary attacks

The most common type of password attack is simply a high-speed guessing game.

These attacks involve starting with an exhaustive list of possible words (including names, profanities, acronyms, and more) and perhaps a few rules to try interesting and common ways that people try to obfuscate words. They calculate the hash of each guess and if it matches what was found in the compromised database of account information that they're working against, they've figured out the password for that account.

As we'll see in a moment, it's easy for hackers to make an amazing number of guesses is a short amount of time.

That's why you're not using that kind of password, right?

That's why a password created from a totally random combination of characters is best; it forces hackers to move on to a true brute force attack to gain access.

Brute force attacks

Computers are fast. In fact, the computer on your desk is so fast that it's ability to do simple operations is measured in terms of billions of operations per second.

Creating a password hash is not a simple operation on purpose. However, it's still something that on most machines today can be done very quickly. Spread the work over a number of machines - perhaps a botnet - and the amount of processing power that can be thrown at password cracking is amazing.

The net impact is that it's now feasible to calculate the encrypted hash values for all possible eight-character passwords comprised of upper and lowercase alphabetic characters and digits.

62 possible characters (26 lower case, 26 upper case, 10 digits), in each of the eight positions gives us 221,919,451,578,0902, or over 221 trillion, combinations.3

---

2 OK, OK. Technically, the number is actually 221,919,451,578,090 + 3,579,345,993,194 + 57,731,386,986 + 931,151,402 + 15,018,570 + 242,234 + 3,844 + 62. When we also add in the possibilities of seven-

This seems like a lot, until you realize that an off-line attack, which is easily performed once you've stolen a database of usernames and encrypted passwords, could be completed in a few hours. (This assumes technology which can "guess" something like 10 billion passwords per second - which for those performing these kinds of attacks is quite possible.)

It doesn't matter what your password is; if it's eight characters and is comprised of upper and lower case letters and numbers, the hackers now have it - even if it was hashed by the service that they stole it from.

Why 10 is better and 12 better still

As we've seen, eight-character passwords give you over 221 trillion combinations, which can be reasonably brute force guessed offline in hours.

Ten characters gives you over 850 quadrillion (853,058,371,866,181,866), and the offline brute force guessing time would be measured in months.

Twelve characters gives you over three sextillion (3,279,156,381,453,603,096,810), where the offline brute force guessing time would be measured in centuries.

That's why 12 is better than 10 and both are better than eight.

What about special characters?

I did leave out special characters; it's true.

Let's say that the system that you're using allows you to use any of 10 different "special characters" in addition to A-Z, a-z and 0-9. Now, instead of 62 characters, we have 72 possibilities per position.

That takes us to 700 trillion possibilities.

Compare that to sticking with the original 62 letters and numbers, but adding only a single character to make it a nine-character password.

That takes us to over 13 quadrillion possibilities.

---

character passwords, six, five, four, and so on. I'm not doing the math. It's around 225 trillion.

3 Many of the numbers and attack estimates here come from or are based on GRC.com's excellent Password Haystack page. Included there are links to an excellent Security Now! podcast segment discussing password length and how size really does matter.

Yes, adding and using special characters makes your password better, but significantly better yet is to simply add one more character.

So add two. Or four. 

Shouldn’t services fix this and do better?

Absolutely, they should. And many do.

As I've stated above, passwords shouldn't be kept in plain text anywhere by the service at all. And yet, some do.

There are techniques that make the brute force attacks significantly harder ... and yet many use techniques which are easier than the example I use above.

There are services that do a great job of keeping your information secure. There are also services that don't. The problem is that you really can't be certain which is which.

To be safe, you have to act like they're all at risk.

The bottom line

The bottom line for staying safe is simply this:

- Don't trust that the service that you're using is handling passwords properly. While many do, it's become painfully clear that many do not, and you won't know which kind that you're dealing with until it's too late.
- Use longer passwords; 10 characters minimum, 12 if at all possible.
- Use a different password for each different site login you have. That way a password compromised on one service won't give hackers access to everything else.

Even the best eight character passwords should no longer be considered secure. 10 is "good enough for now" but you really should consider moving to 12 for the long run.

Related Articles on Ask Leo!

- What's a good password? Good passwords are hard to crack and hard to remember. As a result, many people don't use really good passwords, even though they should. We'll look at what makes a good password, and some ways to make them easier to remember.
- Is changing my password enough? Changing your password is a common response to security breaches. Unfortunately, it may not be enough to recover.

- Dictionary Attack: What is it? A dictionary attacks is a common brute force way of achieving a goal. The goal of a dictionary attack might range from compromising your system to simply sending spam.

Article C4844 - June 13, 2011

Phishing? What's Phishing?

> Phishing is a way that internet scammers trick you into providing your personal and financial details. Phishing opens the door to identity theft, and more.

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?

•

Phishing is a word you hear a lot in the news these days, and this question brought it to mind.

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 account or identity theft and all the hassle that entails.

Here's how it works:

The bad guys, or "phishers", create an 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 that also looks very official and proper. At that site you're then prompted to enter all your personal information, typically 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 never ask you for your private information via email. It's that simple.

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

http://www.ebay.com/

That's a link to eBay, right?

No, it's not.

In most browsers if you hover the mouse over that link, you'll see that it does not go to eBay at all, (you'll see the real destination either in popup

text, or in the browser's status line near the bottom of the window). But it certainly looks like it does. If you click on it, you'll be taken somewhere else entirely.

These same tricks work in HTML formatted email, which is what most of these phishing attempts use.

In the example above, it's obvious you're not at eBay if you click through. But if the destination site also looked like eBay, you could be fooled into thinking it was legitimate. Even more so, if the domain "kinda sorta" looked like an ebay domain. Maybe something like http://www.ebay.verification.somerandomservice.com - you might look at that and see the "www.ebay" and stop reading - and yet it's the stuff at the other end of the domain name - somerandomservice.com in this example - that tells you the most about where that link might really go.

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 be secure. That means it should begin with https:. If the target destination for anything that claims to be secure, or account validation related 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 the link - do not click on it. Never click a link in the email itself.

If you must satisfy your curiosity, or just want to double check what might be going on 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 or contact their support line or search their support site. Trust me, they'd much rather have you ask than have to deal with the possibility of identity or account theft.

For another approach to phishing that uses only email, check out Is Windows Live Hotmail about to close my account? I also discuss there some additional signs that an email message may not be legitimate.

Related Articles on Ask Leo!

- Can I prevent phishing attacks by using a bookmark? You can prevent phishing attacks several ways; the most common is to never click on an emailed link. Bookmarks can be also be used to prevent phishing.
- Why does my anti-malware software say a link is suspected phishing? Anti-malware software examines links to see if they go where they claim to go. The problem is that valid links can be mislabeled as phishing attempts.

Article C2276 - November 28, 2009

Is changing my password enough?

> Changing your password is a common response to security breaches. Unfortunately, it may not be enough to recover.

I regularly hear from people who've had their email or other online account compromised, who somehow are able to recover access to it and change their password, only to have the account stolen almost immediately again.

The problem is actually quite simple, though the solution is a bit of work.

First, you have to realize that while someone else has access to your account they have access to everything related to that account.

Second, you have to realize that because of that, changing your password just isn't enough.

•

You authenticate with most online systems by providing a user name and a password. Your username might well be publicly visible, but your password should be known only to you.

Most systems also provide a mechanism whereby you can recover or reset your password should you forget it. They use a variety of means, but they all boil down to the same thing: they use one or more additional pieces of information to validate that you are who you say you are, and then reset or reissue your password.

It's those "additional pieces of information" that present the greatest risk once your account has been compromised.

Let's look at some examples of what I mean, why they're a risk, and what you should do about each in addition to changing your password.

- Email address or alternate email address.

  Many if not most online accounts require your email address. In the case of an email account (like Hotmail, Gmail or the link) there's often an "alternate" email address. Systems often provide the ability to send a password reset message to that email address of record

should you lose your password. Since only you could have set it up, by definition that email address should be yours.

Once your account has been compromised, a smart hacker will immediately go in and change that email address to one that he has access to. That way, if you request a password reset, he'll get it, not you. Similarly, if you change the password, all the hacker has to do is request a password reset, and he'll regain access to the account.

What you should do: once you've regained access to your account, immediately verify that all email addresses associated with that account are yours. If they aren't change them right away.

- "Secret" questions and their answers

  Many systems have you set up answers to questions as a second layer of security should you lose your password. The answers are typically to questions that only you should know such as your mother's maiden name, your first pet or your favorite teacher. If you forget your password, many systems then simply ask you one or more of these questions, If your answer matches what you set up originally, then you must be who you say you are, and you'll get your password reset and/or account access.

  I put "secret" in quotes because this is one of the problems with the technique: quite often the answers aren't secret at all. It's recently been shown that even a little browsing on social media sites of which you happen to be a member can often tell potential hackers a great deal about you, including many of the answers to these so-called secret questions.

  Once a hacker has access to your account, it's not uncommon for the answers to your secret questions be visible to him. If he's smart - and some are - one of the first things he'd do is jot down the answers to all your secret questions, or change them to his own. That way, should you regain access to the account and change the password, he can just invoke the password recovery mechanism and regain access himself.

  What you should do: once you've regained access to a hacked account, change all your secret answers immediately. Even if they've been untouched, the attacker could simply have written them down and know them all. Change them to something new - ideally answers that are completely unrelated to the questions, but that you'll be able to remember in the future.

- Mobile/Cellular information

  Some providers allow you to specify your mobile number as part of your account information, and then can SMS or otherwise contact you via that information to perform password resets and more.

  By now you probably realize that once a hacker has access to your account they can change that number to be their own. Any mobile-based account recovery attempts are now redirected to the hacker.

  What you should do: as soon as you get back into your hacked account, change or remove this information.

- Billing information

  It's rare, but some systems will use billing information, such as a credit card number already on file, or your billing address in account recovery and validation attempts.

  If you have this kind of information on file, a) a hacker can start using it, potentially racking up charges that you may, or may not be liable for, and b) a hacker can change it so that if it's used for account recovery purposes it's the hacker that that'll regain access and not you.

  What you should do: change or remove this information as soon as you get your account back, and check with your credit card provider immediately for any improper charges.

By now you should see a distinct pattern: any and all information that can be used to recover your account should be validated, removed or changed the instant you get your account back. That includes personal information, PINs, secret questions and answers, alternate email addresses and more - anything that the system you're dealing with might use for account validation and recovery.

If you don't, and the individual that hacked your account has even half a clue, it's very possible that you could recover your account only to find it hacked again within hours or even minutes.

Related Articles on Ask Leo!

- Would you please recover my password? My account has been hacked or I've forgotten it. I'm asked daily to reset lost passwords,

recover hacked email accounts or retrieve lost information in them. Here's my answer.

- Someone has stolen my email account. What can I do to get it back? The outlook is grim if your email account has been stolen, but there are a couple things that you can try to do to recover it.
- What's a good password? Good passwords are hard to crack and hard to remember. As a result, many people don't use really good passwords, even though they should. We'll look at what makes a good password, and some ways to make them easier to remember.

Article C3913 - November 6, 2009

Backing Up

Has your computer ever crashed just seconds before hitting the "save" button? Then you understand how frustrating losing all your data can be. Now imagine losing your family photos, your tax returns-every last one of your important files. Permanently. In a perfect world, data would never be lost, hardware would never fail, and we'd never accidentally permanently delete something. Well, news flash: We do not live in a perfect world. With more than 66% of internet users having suffered some sort of major data loss, it's a simple concept: If you use a computer, you need to backup your data. Backups are crucial to protecting ourselves from everything from virus infections to hardware failure. Adhering to the ever-popular "it'll never happen to me" mantra, is a guaranteed recipe for disaster.

What backup program should I use?

> Backing up your computer's data is critical. What program should you use? There are many, but the best is whichever one you actually will use.

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.

So let me ask you this: do you know how you'd recover your data should everything on your computer suddenly disappear?

•

In order to choose what's going to work best for you, there are several questions you need to ask yourself.

Do I want to put a lot of thought into this? If not - and most don't - 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.

In addition to a drive, you'll need backup software. Many external drives will actually come with backup software of some sort so that's often a good place to start. If you elect to purchase backup software there are many good choices - I personally use and recommend Acronis True Image for most home users. Starting with Windows 7 the backup program included with the operating system is also worthy of consideration.

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 - which 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 a great deal of diligence on your part because anything you don't specify that needs to be backed up 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 local 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.

Might on-line backup be an option? If the amount of data you're backing up is manageable, and your internet connection is relatively fast, then an on-line backup system such as Carbonite, Mozy, JungleDisk or others may well be worth considering. These systems install software on your machine that backs up your critical files to secure servers "somewhere" on the internet, thus getting you both data backup as well as off-site backup at the same time. In addition, some services then allow you to access your backed up files from any machine connected to the internet. For large backups, such as full image or system backups, this approach is typically impractical due to upload speed and storage size limitations.

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; one example might be 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 a leveraging a tool I wrote many years ago called SyncFile, in addition to using Acronis True Image.
- I'm very comfortable re-installing everything so with the exception of only one machine - my primary desktop - I backup only my data. My desktop machine gets a monthly full backup and a daily incremental using Acronis.
- I have several machines on my LAN and in the middle of the night there's 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. Since I have servers at a data center half-way across the country, once a week I upload snapshots of my data as encrypted packages. In the past I've had computers at two different physical locations, and used two external drives: each location backed up to an external drive and roughly once a week the drives would be swapped.
- As I mentioned, I do have external servers and web sites as well. I've been careful to ensure that the servers, as well as the files that comprise the web sites, are all 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.

Related Articles on Ask Leo!

- How to Backup A series of articles and videos walking through the steps to backup - and restore - your computer.
- How do I backup my computer? Backing up your computer is an important step to avoiding data loss. We'll look at what it is, and give a suggestion for average users.
- Can't I just copy everything instead of using a backup program? It's tempting to just use file copy tools to backup what you think you

need. But if you're not careful, you could easily miss something very important.

- Can I do my backups over the internet? Backing up to a service or server across the internet can be a useful part of a larger backup strategy, but the technique does have important limits.

Article C1894 - November 22, 2009

How did you backup while on your trip?

I took technology with me on my three week vacation, as most of us do. It was an opportunity to think through how best to prepare for the worst.

My wife and I recently returned (or rather are returning - I'm writing this at 31,000 feet somewhere over the Pacific Ocean) from a 3 week trip to Australia and New Zealand. Being who I am, and doing what I do, both for fun and for business, you can imagine that some technology accompanied me: my laptop and my digital camera.

Prior to leaving I put some serious thought into exactly how best to ensure that I was prepared for various misfortunes that can happen while on the road. Given how often I cajole, preach and harp on "backup, backup, backup!" I also needed to set a good example as well - nothing would be more embarrassing in my position than suffering catastrophic data loss that could have been prevented by some form of backup.

Understanding what I needed began with a simple assessment of what data I would have, what might go wrong, and understanding the relative priorities of it all.

•

Even just taking a laptop and a camera on a trip means you're taking a lot of data with you. Operating systems and applications of course, but also programs, the data used by those programs, email, photographs and more.

As I looked at the data I would carry and generate while on my trip, I came to a realization that there was really only one class of information that was truly and irrevocably irreplaceable: the photographs I would take on the trip itself.

To make that even more scary I frequently get questions that begin with "Help! I've lost all my pictures!".

Clearly they warrant some serious consideration.

Literally everything else could be recovered - at cost or inconvenience, perhaps, but it could be recovered. My laptop and camera could be replaced. The operating system and applications could be reinstalled. The data carried with me was backed up at home prior to leaving. My email is backed up on both my own email server and Gmail. The only thing I would

truly lose if I lost both my camera and laptop would be copies of any email I sent after leaving home (a loss I was willing to accept), and all my trip photographs (a loss I was not willing to accept).

My backups took two forms.

External Hard Drive

When I travel I carry with me a Seagate FreeAgent Go 500 gigabyte external USB drive. At the end of each day I do a system backup. In my case that's a custom script, but a traditional daily incremental backup using any of a number of backup tools would have been just as appropriate. This duplicates everything that changed since the prior backup. On this trip that means that photographs downloaded from my camera are copied to this backup daily.

I also took the extra paranoid step of making sure that the external hard drive and my laptop never traveled together: as I type the hard drive is in my luggage, and my laptop with me in the airliner cabin. If I lose my luggage, I still have my laptop. When we left for day trips where the laptop remained at the hotel, I threw the hard drive in my backpack that came with me. If my laptop were to be stolen, I'd still have my backup.

The thinking here is something along the lines of off-site storage. It's all well and good to have a backup, but if that backup gets stolen, lost or destroyed along with the original, it does you no good. Hence, I tried to make sure that when practical the laptop and the backup drive were in the same place together as little as possible.

But my paranoia didn't end there.

Postal Mail

This was a pretty special trip for us, and the pictures I was to take would be incredibly important keepsakes. Even though remote, the possibility of losing both the laptop and hard drive - and all my photographs - was something I didn't want to let happen.

One approach that I discarded early was to upload everything daily to my own server - I have lots of space there after all. Unfortunately, internet connectivity was to be questionable, slow and often expensive. It just wasn't practical to upload what in the end turned out to be roughly 24 gigabytes of photographs (roughly 2,300 images).

Instead, I went "old school".

Before I left I purchased 10 4-gigabyte compact flash cards and prepared self-addressed envelopes in which to mail them home. At the end of our stay in each city, I'd copy the accumulated photographs to a CF card, and drop it in the mail. Some of my photographs would be home before me,

and the rest would trickle in shortly after my return. Even if the absolute worst happens and we lose everything short of our lives, we'd still have our pictures.

A Note About Sequencing

The rule of thumb when considering important data is to never have only a single copy - always have a backup.

I kept that in mind even as I downloaded photographs from my camera to my laptop.

A common approach is to "move" photographs - deleting them from the camera as they are placed on the laptop, so as to make room on the camera's memory card for the next day's pictures. But that still results in only one copy of the pictures, and during a copy operation that can, in some cases, be destructive (if a hard drive goes bad during a move, for example, the file being moved could conceivably be lost).

My approach was to follow this sequence:

- Copy the photographs from the camera's memory card to my laptop. This immediately created the desired "two copies of everything".
- At some point, I would backup the laptop - effectively creating a third copy of the pictures on the external drive. (One in the camera, one on the laptop, and one on the external drive.)
- Only then would I delete the photographs from the camera's memory card.

The result: two copies as soon as possible, and never less than two copies thereafter.

A Note About Security

I've not talked about security, because this is primarily an article about backing up, but the two cross paths, as you might expect.

The question to be answered is simply this: will someone have access to my personal data if:

- my laptop gets stolen?
- my backup drive gets stolen?
- one of those compact flash cards I dropped into the mail gets intercepted?

Long time readers will know at least one of my solutions of course: TrueCrypt, and will recognize the other: 7-Zip.

My laptop's data is encrypted in a TrueCrypt volume. Without the pass phrase, it's so much random data to a thief.

My backups happen to use 7-Zip, and they're password encrypted with an exceptionally strong password.

The surprising one as I was setting all this up was the compact flash memory cards that I was mailing to myself. I decided that I didn't really want some random person to have access to my photographs should the memory cards fall into the wrong hands. So, rather than actually containing the photographs directly, each 4GB memory card instead contains a single file: a 4GB encrypted TrueCrypt volume, inside of which are the photographs I'm mailing home. Once again useless without the pass phrase.

Are You Protected?

I'm sure that some of you will consider the approaches that I've taken excessive, and I can understand that. Others may have different ideas to achieve similar results that work better for them.

I share my paranoia and my approach for two reasons:

First: you would not believe the number of people I hear from that have lost their precious photographs because they've not performed even the most basic of backups - sometimes never even downloading from their camera. If you take away nothing else, take away this: two copies of everything, and as soon as is practical.

Second: even when you do backup regularly, it's easy to overlook scenarios like losing both your original and backup, which is especially easy while traveling - often when what you might lose is more valuable than ever. It's worth thinking through the scenarios, the priorities and importance of what you have, and taking appropriate measures.

Losing all your vacation photos can be painful, and taking the trip again just isn't the same - even when it's possible.

Related Articles on Ask Leo!

- TrueCrypt - Free Open Source Industrial Strength Encryption TrueCrypt provides a solution for encrypting sensitive data - everything from portable, mountable volumes to entire hard disks.
- 7-zip file archiving utility There are many win ZIP archive programs. 7-Zip is free zip software, full featured, compatible and the zip software I recommend.
- What backup program should I use? Backing up your computer's data is critical. What program should you use? There are many, but the best is which ever one you actually will use.

Secure Your Mobile Connection

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 WPA security enabled if anyone can walk within range.

How do I use an open WiFi hotspot safely?

> Open WiFi hotspots at coffee shops, airports and other public places are opportunities for hackers to steal information. I'll review how to stay safe.

I've returned to the same coffee shop where I was a few months ago when I noticed that my email had been hijacked/hacked. This time, I'm using my phone, but the last time when I noticed the hack, I was using my computer and doing email over an open-internet, free WiFi network.

Do you think that could be the source of the problem or just a coincidence? I'm still afraid to do email from here.

•

It definitely could have been. Unfortunately, it's hard to say for sure and it could have been something else unrelated.

As we can't really diagnose the past, let's look ahead instead.

It absolutely can be safe to do email from a coffee shop or any other location that provides unsecured or "open" WiFi. In fact, I do it all the time.

But you do have to make sure to follow some very important practices to ensure your safety.

•

Turn On The Firewall

This is easily and frequently overlooked.

When you're at home, you may use your router as your firewall and keep the Windows or other software firewall on your machine disabled as redundant. That works well, as the router stops network-based attacks before they ever reach your computer.

When you're on an open WiFi hotspot or connected directly to the internet via other means, that software firewall isn't redundant. In fact, it's required.

Make sure that the firewall is enabled before connecting to an open WiFi hotspot. Various network-based threats could be present on an untrusted connection, and it's the firewall's job to protect you from exactly that.

Consider Not Using Free WiFi

As I said, it can be safe to use open WiFi, but it's also very easy for it to be unsafe.

The solution that you used while you were at that same coffee shop (and asked me about in this question) is a very common and solid one: use your phone instead.

While it is technically possible, a mobile/cellular network connection is significantly less likely to be hacked. I use this solution when I travel.

Most mobile carriers offer one or more of the following options:

- Use your phone. Many phones or other mobile devices, such as iPhones, iPads, Droids, Blackberrys and others, are quite capable email and web-surfing devices, and typically do so via the mobile network. (Some can also use WiFi, so be certain that you're using the mobile broadband connection for this option to avoid the security issues that we're discussing.)
- Tether your phone. Tethering means you connect your phone to your computer - usually by a USB cable, but in some cases, via a Bluetooth connection - and the phone acts as a modem, providing a mobile broadband internet connection.
- Use a dedicated mobile modem. Occasionally referred to as "air cards", these are USB devices or PCMCIA cards that attach to your computer and act as a modem, providing a mobile broadband internet connection, much like tethering your phone.
- Use a mobile hotspot. In lieu of tethering, many phones now have the ability to act as a WiFi hotspot themselves. There are also dedicated devices, such as the MiFi, that when turned on, are simple dedicated hotspots. Either way, the device connects to the mobile broadband network and provides a WiFi hotspot accessible to one or more devices within range. When used in this manner, these devices are acting as routers and must be configured securely, including applying a WPA/WPA2 password so as not to be simply another open WiFi hotspot susceptible to hacking.

I travel with a MiFi, and also have a phone capable of acting as a hotspot as a backup. I find this to be the most flexible option for the way I travel and use my computer.

Secure Your Desktop Email Program

If you use a desktop email program such as Outlook, Outlook Express, Windows Mail, Windows Live Mail, Thunderbird or others, make certain

that it's configured to use SSL/secure connections for sending and downloading email.

Typically, that means that when you configure the email account in your email program, you need to:

- Configure your POP3 server for downloading your email selecting "SSL", "TLS", or "SSL/TLS" security option, and usually a different port number, such as 995 instead of the default 110.
- Configure your SMTP server for sending email selecting "SSL", "TLS", or "SSL/TLS" security option, and usually a different port number such as 26, 465, or 587 instead of the default 25.

The exact settings and whether or not this is even possible depends entirely on your email service provider; you'll need to check with them to determine the correct settings to use. How you configure these settings, of course, depends on the email program that you use.

With these settings, you can feel secure downloading and sending mail using an open WiFi hotspot.

It's what I often do when I don't have my MiFi with me.

Secure Your Web-based Email

If you use a web-based email service like Gmail, Hotmail, Yahoo or others via your browser, you must MUST MUST make sure that it uses an httpS connection and that it keeps on using that httpS connection throughout your email session.

I believe that this might well be the source of many open WiFi-related hacks. I expect that people simply login to their web-based email service without thinking about security and as a result, the username and password are visible to any hackers in range who care to look.

Some email services have "require https", which is an option you should definitely enable. The problem is that of the major services, I trust only Gmail to remain in https throughout the entire session (and even then, you need to take care if you then use other Google services using your Gmail account credentials). Some services will use https for only your login, which is insufficient as your email conversations thereafter could be viewed by others. Other services may "fall out" of https, reverting to unsecure http without warning.

Facebook also falls into this category. Facebook has a "require https" option, but apparently can fall out of https, particularly when various Facebook apps are used.

Any and all web-based services that require you to login with a username and password should either be used only with https from start to finish, or should be avoided completely while you're using an open WiFi hotspot.

Use a VPN

This one's for the road warriors. You know them - the folks who are always traveling and online the entire time they do so - often hopping from coffee shop to coffee shop in search of an internet connection as they go.

A VPN, or Virtual Private Network, is a service that sets up a securely encrypted 'tunnel' to the internet and routes all of your internet traffic through it. Regardless of https or not, SSL/secure email configuration or not, as all of your traffic is securely tunneled, no one sharing that open WiFi hotspot can see a thing.

This service typically involves a recurring fee. As I said, they're great for road-warriors but probably overkill for the rest of us as long as we abide by the other security steps described above.

Use Different Passwords

Finally, it's a good idea to keep the passwords of the accounts that you access different from each other and, of course, secure.

That way, should one account be compromised by some stroke of misfortune, the hackers won't automatically gain access to your other accounts that they may then learn of.

•

As you can see, it's unfortunately easy to get this stuff wrong. When that happens, that guy in the corner with his laptop open could be watching all your internet traffic on the WiFi connection, including your account credentials as they fly by.

And when that happens, you can get hacked.

Fortunately, with a little knowledge, forethought, and preparation, it's also relatively easy to be safe.

Related Articles on Ask Leo!

- How do I stay safe in an internet cafe? When connecting to the internet in an internet cafe, hotspot or other public connection you could be opening yourself up to serious security issues.

- Is cellular broadband more secure than WiFi? Cellular is a popular internet connection alternative. As with any connection it's important to understand the security ramifications and tradeoffs.
- Is it OK to use this random wireless network that I just found? When scanning for wireless connections you may find several that are unknown yet and appear open and available. Using them is risky. Very risky.

Article C4790- April 10, 2011

Can hotels sniff my internet traffic?

> More and more hotels are offering both wired and wireless internet, but along with those connections comes a security risk most folks don't consider.

My friend's husband has been getting into her email even though she's not given him her password. He has confronted his sister about an email and when asked how he got into the email he says that where he works (A large hotel chain) they have a program that searches emails for keywords and brings info up. Could that be true?

•

Yes.

Hotel network security is one of the most overlooked risks travelers face. And I'm not just talking wireless, I'm talking any internet connection provided by your hotel.

In fact, I'm actually writing this in a hotel room, and yes, I have taken a few precautions.

It's a topic c|net blogger Michael Horowitz has also written about: Ethernet connections in a hotel room are not secure and the title says it all.

I'll put it another way: hotel internet connections are just as unsafe as an unsecured wireless hotspot.

Any hotel internet connection.

There are two basic issues:

Your ISP can see everything you do. When you're in a hotel, that hotel is your ISP. They provide the connectivity, the routers and other equipment that connects you to the internet. As a result, they have the ability to monitor any and all traffic on the network. And you need to realize that it's their network that you're using - they own it, they control it and they have the right to monitor its usage. And, as you've seen, employees can abuse that power to go snooping.

Your neighbors may also be able to see what you're doing. Depending on exactly how the network is configured, it's possible that you and the rooms around you are connected through a hub. The "problem" with a hub is that it's a dumb device - it sends everything it gets to everything connected to it. So when you send data through the hub, not only does the upstream internet connection see the data, as you want, but that data

is also sent down the wires to your neighboring rooms. Any computers there should ignore it, but it's there for the taking if they do not. This is exactly like connecting via an open WiFi connection where anyone in range can "sniff" your internet traffic.

There's actually a third more sinister problem where an intentionally malicious hotel guest "poisons" some of the information used to route internet traffic and inserts his computer into the middle of your conversations.

So, what do you do? What do I do?

In a word: encrypt.

This basically boils down to following all the same steps one might take to stay safe in an internet cafe:

- Use a Firewall: make sure your Windows or other software firewall is enabled.
- Use https: only access sensitive websites, for example, banking, but also things like web mail, using an https connection. Most banks are secure by default, most web mail is not.
- Encrypt your email: if you're using a normal email program and downloading your email via POP3 or IMAP, or sending your email via SMTP, then you need to make sure that those connections are encrypted. Check with your email provider for the appropriate settings.

Now there's one more aspect to internet usage that often gets overlooked, and that's simple web browsing.

For example, as I sit in this hotel room it's possible that if I didn't take appropriate precautions my neighbors, were they technically savvy enough, could monitor which web sites I'm browsing. In fact, if any of those web sites require me to login, they could potentially see my login information and password. Recall that I said most web mail is not encrypted using https? That's exactly what I'm talking about here: if you connect with a normal http connection any usernames and passwords you might enter are transmitted in the clear and are visible to anyone who has enough access to sniff your internet traffic.

Once again, the answer is a single word: encryption.

The most common solution is a VPN or virtual private network. There are several commercial services tailored specifically to folks who travel a fair amount. The way it works is simple; after signing up you create a VPN connecting to their servers and all your internet traffic is encrypted and routed through them. At the service, the data is decrypted and sent on to its final destination. Anyone in between - meaning your hotel guests, staff

and whoever else might be peeking, cannot see your data. More correctly they can see your data, except it's encrypted and total gibberish to them.

So what do I do?

Well, I run Thunderbird as my email program, downloading and sending via POP3 and SMTP. I've configured each to connect to my mail servers using an SSL encrypted connection. My mail is secure.

For unencrypted (http without the s) websites, I establish an encrypted tunnel - think of it as a kind of partial VPN - to my server.

For encrypted websites (https with the s) I need do nothing, other than make sure that the connection remains "https" as I navigate from page to page.

My web surfing is secure.

Since I'm not using a "true" general purpose VPN, as I outlined above, I have to be careful about instant messaging programs. My approach to date has been to connect via remote desktop (which is encrypted) to one of my machines at home and run the instant messaging programs there. In fact, I use this technique for everything that access the internet that isn't web surfing, email or already inherently secure.

Is it all overkill? I think not. With more and more computers and more and more public internet access, hackers and thieves need very little in the way of technology to steal all sorts of sensitive information. Are they doing it here and now? I'd guess not.

But I'm not so sure of that guess that I'd let down my guard.

Better secure than sorry.

Related Articles on Ask Leo!

- How do I stay safe in an internet cafe?
- Can hackers see data going to and from my computer?

Article C3291 - February 14, 2008

Can hackers see data going to and from my computer?

> In some instances, it might be possible for hackers to see data going to and from one's computer. Sometimes it matters, but sometimes it doesn't.

I've heard that instant messages through AOL/Yahoo/MSN can be read by hackers that "sniff" the messages leaving my network. Is this true?

•

Yes.

It's actually true for all the data that comes and goes on your internet connection: web pages, emails, instant messaging conversations and more.

Most of the time it simply doesn't matter. Honest.

On the other hand, there are definitely times and situations when you really do 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 across the internet, it actually travels across many devices each of which can "see" the data.

Sounds scary.

The good news is that's actually pretty 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 that DSL connection might watch your traffic, but random machines out on the internet would have an extremely difficult time tracking it down.

It's not something I worry about much at home.

However, there are scenarios that you should be very aware of.

- Wireless access points operate much like a hub. Any wireless adapter within range can see all of the network traffic in the area. Visited any open (meaning not WPA-encrypted) wireless hotspots

lately? Anyone in the coffee shop or library, or even just outside on the street or a nearby building, could be sniffing your traffic.

- Hotel or other third-party provided internet connections are also vulnerable, since you have no idea what, or who, is sharing or watching your connection. It's possible that you're on a hub, and the room next door or down the hall could be watching your traffic, or it's possible that the hotel staff themselves are tapped into the internet traffic to and from all the rooms.
- Landlord-provided internet connections, or those provided by or shared with a roommate or housemate fall into the same category: whomever set it up could very easily be watching the internet traffic going to and from the connection(s) that they provide you.
- Your connection at work can also easily be monitored by your employer. In fact, the only difference between your employer and a hotel or landlord provided connection is that in most places the employer snooping on your use of their connection is legal, whereas the others typically are not.

So, what to do?

Aside from avoiding the situations listed above where this kind of eavesdropping is not only possible but often downright easy, the answer boils down to encryption of one form or another.

If you can, make sure that your own wireless hotspots are configured to use WPA2 encryption. (WPA if that's all that's available. There's no point in using WEP, as it is trivially cracked.) This way your wireless connection is secure. Even if someone does sniff and see your data going by, all they'll see is encrypted noise.

If, as in most of the examples above, you do not have control over the wireless connection, and have no control over the actual connection to the ISP, then additional steps are necessary.

As a start, if you're on the road you might simply wait until you're home to access sensitive sites like online banking or others.

In terms of technologies to help keep you secure, the list includes:

- https (as opposed to http) connections are encrypted. Even traveling over unencrypted media like wired connections or open WiFi hotspots, the https protocol securely encrypts the data that is being sent to and from the web site being accessed. In addition, it also provides an additional level of security that the site you think you are connecting to is, in fact, that site. Not all sites support https (Ask Leo! is one such example) but sites that provide you with access to any potentially sensitive information - including your web-

based email - should provide an https connection, or should be avoided.

- Secure email connections should be used with your desktop email programs such as Outlook, Thunderbird, or any program on your computer that uses POP3/IMAP and SMTP. By default most email services have you configure your email connection for downloading your email using unencrypted protocols. Many now offer the ability to specify encrypted equivalents. If you're in any of the situations above, only encrypted protocols should be used.
- VPNs or virtual private networks are technologies that can be used to secure your entire internet connection by creating an encrypted "tunnel" to a third party. All of your internet traffic goes to this trusted third party - encrypted - and from there it connects to the rest of the internet. All your internet traffic traveling between you and that third party is safe from sniffing by virtue of being encrypted.

  The "third party" might be your place of work, if they offer such a thing, and as noted above, if you trust them. Other alternatives include services like HotSpotVPN which are targeted at folks traveling a lot who make regular use of open public WiFi and other fundamentally unsecure internet connections.

In general, when people ask about the security of their data it falls into one of two broad categories:

Privacy and Security or folks who are concerned that they're being spied on. My general response is that most of us as individuals just aren't that interesting, and it is rarely anything to be concerned about.

Opportunistic Theft or situations where someone's looking not specifically for you or me, but rather for someone who's allowed their bank, email or other secure information to be available for stealing. By leaving information available out and available to thieves, you can become a victim.

The good news is that the advice and technologies above go a long way to addressing both issues. The bad news, of a sort, is that it's still your responsibility to make sure that you're secure and using them appropriately.

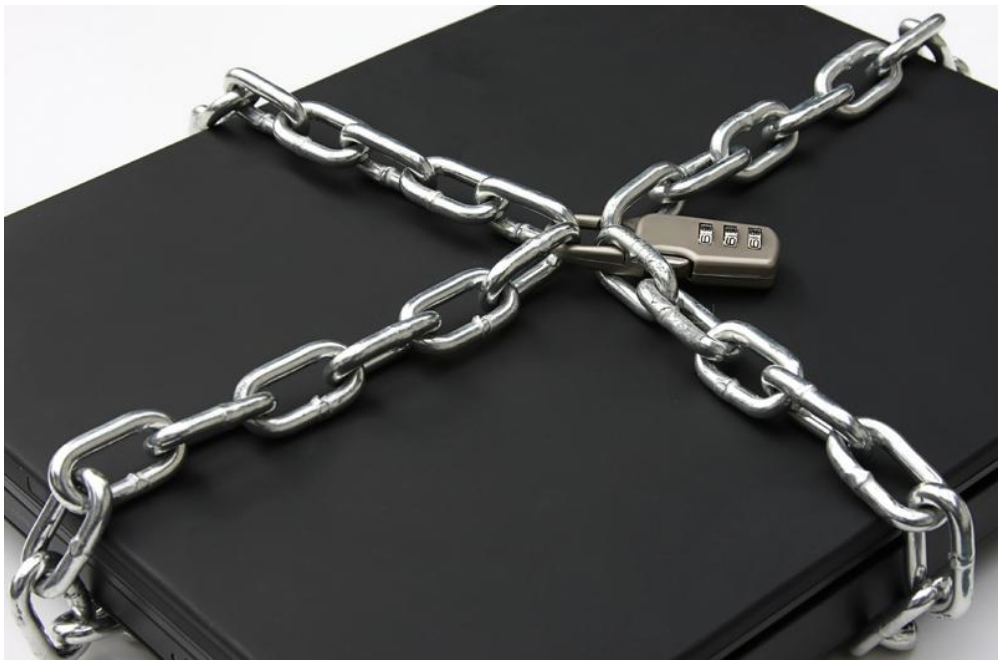
Related Articles on Ask Leo!

- How do I stay safe in an internet cafe?
- Can my ISP monitor my internet usage? Your ISP controls your internet connection and it's easy for them to monitor the data you send and receive. The question is, why would they bother?

- Can hotels sniff my internet traffic? More and more hotels are offering both wired and wireless internet, but along with those connections comes a security risk most folks don't consider.

Article C2290 - January 9, 2010

Don't forget the physical



An old computer adage:

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

All of the precautions I've listed so far 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?

> Laptops are portable, convenient and easily lost. When lost, all the data could easily be available to the finder. Encryption is the answer.

I travel a lot, and have sensitive data on the laptop I take with me that I need as part of my job. But I'm in fear of losing the laptop and that this data will fall into the wrong hands. What do you suggest?

•

I know how you feel. I also have sensitive information on my laptop that I would prefer not to fall into the wrong hands. I can handle losing the laptop, but thinking about the data in the wrong hands ... well ... that would be bad.

I do have a solution that I've been using for several years now, and it turns out to be fairly easy, secure, and free.

•

Now, naturally, you can encrypt your data using various archiving tools that allow you to assign the resulting file a password. The problem is that many are easy to crack, and to be honest, it's a hassle; in order to encrypt a file you have to take care to place it in the archive and erase unencrypted copies, and in order to use a file you need to extract it from the archive.

For some time now, I've been using TrueCrypt. TrueCrypt is free, open source, on-the-fly encryption software. It provides serious industrial-strength encryption while still being fairly easy to use.

TrueCrypt can be used in several ways, the two most common:

- it can encrypt an entire disk volume - such as a USB thumb drive, floppy disk, or an entire hard disk
- it can create an encrypted virtual disk "volume" or container

It's the later approach that I like to use, as it makes it easy to copy entire containers from machine to machine.

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 DEcrypted and anything you place there is ENcrypted.

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.

While the encrypted volume is mounted, its contents are visible in their unencrypted form, and can be accessed by any program you might want to run.

The trick is to never mount the drive automatically. When your machine boots up, "P:", for example, would be nowhere to be found. The file c:\windows\secritstuf would be present but only visible as encrypted 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:

- The password or passphrase you choose is the weakest link. Encryption does not make a bad password any more secure. If you choose an obvious passphrase, 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 in some unencrypted form.
- 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 kinda 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 I started this article with, there's no excuse not to take that time, and save yourself some serious grief later if the unthinkable happens.

Related Articles on Ask Leo!

- TrueCrypt - Free Open Source Industrial Strength Encryption
  TrueCrypt provides a solution for encrypting sensitive data - everything from portable, mountable volumes to entire hard disks.
- Can I password-protect a folder? Keeping data on your computer secure is important. Being able to password protect a folder seems an obvious approach. Unfortunately it's not that simple.

Article C2343 - December 12, 2009

Will using an on screen keyboard stop keyboard loggers and hackers?

> Using an on screen keyboard instead of a real keyboard might stop some logging, but there's no guarantee that other techniques aren't also being used.

Will using the on screen keyboard in Vista stop keyboard loggers/hackers?

•

The short answer is very simple: no.

It might stop some, but it's certainly nothing that you can count on.

Let's look at the path of keystrokes from your finger to your computer and see all the various places that your keystrokes can be intercepted and logged.

•

When you type a key on your keyboard, typically a microprocessor within the keyboard does its magic to send a signal up the cable connecting your keyboard to your computer.

And there we reach the very first point of vulnerability. No, not the microprocessor in the keyboard (possible, I suppose, but exceptionally unlikely), but the cable. Or rather what the cable plugs into. Particularly lucrative targets are public computers, where someone comes along and actually installs a physical device between the computer and keyboard; a device that logs every keystroke entered. Sometime later they come back, remove the device and take with it all the information that users of that computer might have entered.

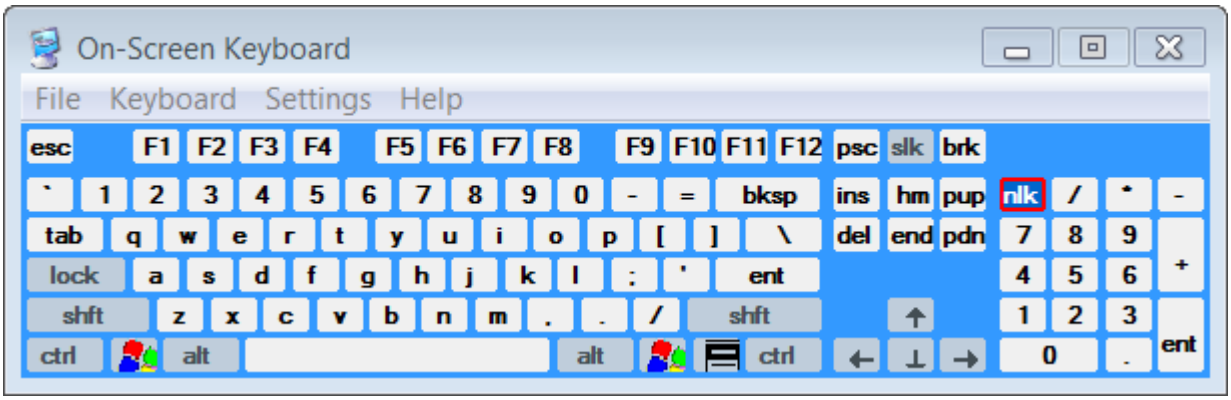
As it turns out, wireless keyboards are worse. Wireless keyboards actually broadcast the keystrokes you're typing. Any receiver within range can "listen in" and record them, and unfortunately "in range" also turns out to be much further than most people think - particularly for a thief with equipment dedicated and tuned to this purpose. While the keystrokes are supposedly encrypted, I recently heard that this encryption is often very easy to crack.

The good news is that your on-screen keyboard actually does protect you against these two specific types of keyboard related threats. By using the on screen keyboard you've avoided touching the actual keyboard you've bypassed any compromise of the hardware.

The bad news is that hardware based keyloggers are rare. Much more common are software based threats.

Once your keystrokes arrive at the computer from the keyboard, they are then processed by a keyboard device driver which (to oversimplify) handles the translation of the keyboard "scan codes" that have come over the wire to the letters, numbers and symbols that Windows applications expect. Keystroke loggers typically insert themselves into the receiving end of this process, so that they get the keystrokes from the keyboard as they are passed on to Windows.

This is where the on screen keyboard scenario gets interesting.



The on screen keyboard application is a "virtual" keyboard. It effectively has its own device driver, and to Windows "looks like" a real keyboard. As a result, the keystrokes it sends onto Windows can quite easily be captured by the same key logging software that's capturing keystrokes from the real keyboard, if that key logger has installed itself into the proper place.

But it gets worse. Much worse, actually.

Let's assume that the keystroke logger is not able to capture the keystrokes from the virtual on-screen keyboard.

A keystroke logger can capture a lot more than just keystrokes, so perhaps it'll capture something else instead.

You use the virtual keyboard by using your mouse to point and click at the image of a key on the keyboard. A keystroke logger could then capture on every mouse click:

- the location of the mouse on the screen
- a screen shot image of the screen, or just the area "around" the mouse pointer

What the key logger has done is captured a series of images showing exactly where you clicked and in what order. In other words, it's captured your virtual keystrokes.

Note that this approach to key logging also bypasses one of the more common so-called security techniques of randomizing the keyboard layout on the screen. You still have to be able to see where to click, and the logger simply logs what you see and where you click, regardless of how the keyboard is laid out.

How big a threat is this?

It depends on whom you ask. In my opinion "normal" keystroke loggers - those that record only keystrokes - are a fairly common threat, and are one part of the reason that anti-malware protection and general internet safety common sense in general is so important. So yes, they're out there.

The real question is how pervasive are these more sophisticated screen capturing keyloggers? It's hard to say, but we do know that malware creators have continued to escalate their attacks, both in technique and in scope. It wouldn't surprise me to see these types of malware increase in frequency.

And I, personally, wouldn't rely on a virtual keyboard of any sort as a security measure.

Related Articles on Ask Leo!

- Is there a way to bypass keyloggers? Keystroke loggers can log a lot more than just keystrokes. We'll look at a couple of ideas for bypassing them, and they chances that you can.
- Spyware: How do I remove and avoid spyware? There are some important steps to take to deal with the ever-present concern of how to remove and avoid spyware.

Article C3617 - January 10, 2009

That's It, And Yet...

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.

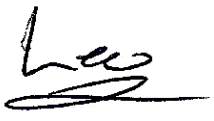
It's a great foundation, a good beginning, but in reality ...

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 ask me a question, any time…



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

About the Author

Leo A. Notenboom has been writing software in various forms since 1976. In over 18 years at Microsoft, he held both managerial and individual contributor roles in a number of groups ranging from programming languages to Windows Help, Microsoft Money and Expedia. Since leaving Microsoft, Leo's been answering tech questions at the extremely popular Ask Leo! web site (http://ask-leo.com) and expending his efforts on various consulting and entrepreneurial projects, such as this book.

Attributions

© Patrimonio | Dreamstime.com (Title Page-art)
© Piksel | Dreamstime.com(Virii and Spyware and Worms… oh my!-art)
© Devonyu | Dreamstime.com(Scan for Viruses-art)
© Bobb | Dreamstime.com(Kill Spyware-art)
© Matthiashaas | Dreamstime.com(Use a Firewall-art)
© Lincolnrogers | Dreamstime.com(Stay up-to-date art)