

7 Easy Steps for **Instantly** Improving Your Online Security

You may redistribute this report --
you may NOT modify or sell this report.

Table of Contents

Table of Contents	2
Background	3
Step 1: Be Spyware Free	3
Step 2: "Phishing" – Don't Be the Catch of the Day	6
Step 3: Protect Your Personal Information.....	7
Step 4: Read the Fine Print	8
Step 5: Hide Your Email Address From Spammers.....	8
Step 6: Switch to a More Secure Web Browser.....	9
Step 7: Take the 60 Second Security Challenge	10
The Next Step	12

© 2005 Doug Partridge – All Rights Reserved

Disclaimer of Warranty / Limit of Liability

The author of this material used best efforts in preparing this material. The author of this material makes no representation or warranties with respect to the accuracy, applicability, completeness or the contents of this report. The author disclaims any warranties (expressed or implied) for any particular purpose, or any consequences arising from the use of this material. The author shall in no event be held liable for any loss or damages.

Trademarks: Windows ® Microsoft Corporation. All trademarks and product names used in this report are properties of their respective owners.

Background

Computer security in the “old days” meant not leaving your laptop unattended or it might get stolen. Today, it’s taken on a whole new meaning and severity.

Certainly the Internet is a wonderful resource which has, in a relatively short amount of time, positively changed most of our lives in one way or another.

However, there is a “dark side” you must be aware of.

Every time you’re on the Internet, you’re intermingling with every type of character imaginable. Some of the more unpleasant types have devised numerous ways to compromise and invade your computer – and ***they don’t require physical access to your computer to do it.***

Some of the threats we talk about are quite serious and if you were previously unaware of them – they might raise your pulse a little. Our intention here is not to frighten you – *but to enable you to conquer these threats, and to avoid being the next Internet “victim.”*

This special report was put together as a public service to help people protect themselves while enjoying the Internet. People with Windows PCs must first know what risks they face, and the simple proactive steps they can take to ensure their online safety and security.

Simply put: *with just a little bit of knowledge and some best practices, we can work together to make the Internet a safer place for all of us. Sound good?*

We hope you enjoy this information and find it useful. If you do, please pass it on to others – so they too can instantly improve their online safety.

Step 1: Be Spyware Free

It seems that not a day goes by without a news story about Internet security threats, with Spyware usually ranking at the top of the list.

Recent Internet studies estimate that between **80-90% of computers are already infected** with one of more forms of **Adware and/or Spyware**. In most cases, *the owners have no idea their computer’s been infected.*

But let's back up a step.

In case you're unfamiliar with "Spyware" – it's monitoring software that's secretly copied onto your computer without your knowledge or consent. How easy is it to get infected with this menace?

Sometimes, all it takes is visiting the wrong website. And just like that, no warning, no pop-up message, **your PC's been infected.**

Spyware¹ comes in "many shapes and sizes" – we'll just focus on the most common and serious forms – i.e., the ones most likely to be encountered.

Keyboard Loggers One of the most dangerous forms of Spyware. Keyboard loggers sit quietly in the background recording characters you type. What are they after? Anything – your accounts, passwords, financial information, emails, etc.

As you can guess, this type of Spyware is closely linked with online identity theft.

Browser Hijackers These are very common. They "hijack" your web browser and essentially take control, and send you to all sorts of undesirable websites.

Since the sites you're taken to are usually hacker controlled websites, you're likely to become even more infected with even more junk.

Adware Adware usually comes bundled with shareware or other suspicious "free" programs.

Its purpose is to monitor and profile your online activities. Why? So you can be assaulted with targeted pop-ups and Spam. Again, once this process starts – it usually snowballs.

¹ Another term you might hear along with Spyware is "Malware." This is just a blanket-term for all malicious software. The name is derived from [malicious] + [software].

Signs That You Are Infected With Spyware

- Your computer runs progressively slower and takes longer to start up.
- Your home page is mysteriously changed to something else (usually something pornographic).
- Starting your browser means spending several minutes fighting to close pop-up windows.
- Strange icons appear on your desktop.
- You notice that new programs were installed on your computer.

How to be Rid of the Menace.

Many assume they are not at risk because they use an anti-virus program -- **please don't be one of these people!**

The bottom line: *everyone with a Windows computer who connects to the Internet for any length of time is at risk (high-speed or dial-up).* Remember the current statistics – **80-90% of computers are already infected with Spyware.**

Have you taken proactive steps to ensure your own PC's safety? If not, chances are you're already infected – how serious is your infection?

The Bottom Line: Spyware is a serious and growing threat – to effectively protect your computer and your sensitive personal and financial information, **you need a dedicated Spyware removal program.**

The **good news** is that there are excellent, high-quality programs readily available to scan your computer and remove junk (and to make sure you're not re-infected).

[Ad-Aware](#) from Lavasoft is a very good Adware/Spyware removal program, and it's free for personal use.

Recommendation: run a full scan at least once a week.

Ad-Aware is good for removing light-to-moderate infections. Heavier infections will require more powerful protection.

[Spysweeper](#) is a top-quality Spyware removal program. As an added benefit, it provides “always on” protection to prevent harmful threats from landing on your PC to begin with.

Step 2: “Phishing” – Don’t Be the Catch of the Day

“Phishing” (pronounced fishing) is when criminals attempt to trick and deceive you into divulging sensitive and personal information by **impersonating** bona fide companies like Citibank, Paypal and Ebay to name just a few.

How is it done?

Criminals impersonate the trusted party by sending out legitimate looking emails warning about a security threat or other serious issue that requires immediate action. The email directs the reader to a website in order to “verify” (actually supply) their account name, password and credit card number.

To complete the deception, criminals will set up a bogus though highly-authentic looking website (complete with company logos and graphics). If the reader completes the process and submits their information, *they’ve just handed over critical information to a criminal.*

To make matters worse since the bogus website is part of the scam – visiting such a site may result in your PC becoming infected with Spyware or other forms of Malware.

Phishing is extremely effective.

Why? In part because of the legitimate appearance of the spoofed email and website, but also because “Phishers” go to great lengths to create a sense of urgency in the reader.

For instance, a Phishing email spoofing a credit card company might mention bogus charges on the readers account. The email will mention that they have 1-2 days to “contest” the charges or they will become permanent. The recipient fearing that perhaps they’ve been the victim of identity fraud quickly goes to the bogus site mentioned in the email, and becomes another Phishing victim.

The Bottom Line: *legitimate companies will never ask you to divulge personal or financial information through an email request. Assume any such request is not only bogus -- but extremely dangerous – delete it.*

When in doubt, call the company in question.

Phishing is a large topic and we've only covered the basics here. An excellent site with more information and actual Phishing samples is <http://www.antiphishing.org>

Step 3: Protect Your Personal Information

Tip: never provide personal or financial information to a non-secure website.

So, what indicates a "secure" website?

Two things to look for are:

1. **https://** ... instead of **http://**... in the address bar
2. A small padlock icon on the lower right-hand portion of your browser window.

The "S" in https stands for "secure" and it means that the information sent between your computer and the website is encrypted.

No need to get overly technical here: encryption is a method for "garbling" information so that only the sender (your computer) and receiver (the website) can understand it. Since all Internet traffic is across public networks, *encryption is essential for protecting your information.*

The Bottom Line: shopping on the Internet can be as safe as shopping anywhere else. When using your credit card online, **always verify that the page in question is a secure page.**

Tip The entire website does not need to be secured – just pages asking for sensitive personal or financial information. Get in the habit of checking for the "**https**" and it will quickly become second nature.

Step 4: Read the Fine Print

This next tip is closely related to the prior one. *“Read the fine print” means that before you hand over any personal information to a website you know exactly how they will use it.*

For instance, will they share or sell your information to third parties? If you give your information to a real estate website, will you suddenly start to receive real estate oriented Spam? This is what you should know before giving over your information.

The Bottom Line: Know and understand how websites will use your valuable personal information by reading their privacy policy. What if they don't have a privacy policy? **Be very cautious about doing business with such a site.**

Step 5: Hide Your Email Address From Spammers

[My Trash Mail](#) provides a wonderful free service in the fight against Spam.

Please visit their site for a detailed explanation of their service, but here's how it works in a nutshell.

There are numerous instances where you must provide a valid email account when registering for a newsletter, Internet forum, etc. Naturally you might be hesitant to use your “real” email address for fear of receiving loads of new and perverse Spam (you've been there, done that).

What you can do instead is use ***anything@mytrashmail.com*** – the account you use does not require a password, and it does not need to be pre-created. Simply put, mytrashmail.com accounts are created *dynamically* or *on-the-fly*.

A few suggestions for using this service:

- These accounts do not have passwords – this is not the place to send any **personal, sensitive or financial information**.
- Since anyone can access any inbox on this system (all you need to know is the account name) use a name no one else would guess – e.g., ***yourname5435@mytrashmail.com***.

- Emails are automatically deleted anytime *between 2 days and 2 weeks* – if there is a particular email you need to hang on to – be sure to forward it to another account.

Of course these accounts don't replace your primary account – but this may quickly become one of your favorite sites.

Note: if you use and enjoy this wonderful free service – please consider showing your support by giving a small donation to the site. Michael Weber, the web master, is kind enough to offer this service free of charge – however, there are costs associated with keeping it live.

Step 6: Switch to a More Secure Web Browser

This means moving away from Internet Explorer (known as "IE" from here out). What's the problem with IE ... well, where do we start?

- ⇒ Here's an article discussing the subject in more detail -- ["Is Your Web Browser Putting You at Risk?"](#)
- ⇒ And here's an excellent site with first person accounts explaining why they dumped IE-- <http://browsehappy.com/>

But back to the question of what's wrong with IE ... it's the numerous security vulnerabilities that seem to constantly plague this program.

Earlier we made the comment that Spyware can be loaded on your computer *"just by visiting the wrong website."* Did you wonder how that could happen?

It's because hackers are able to exploit known security vulnerabilities in IE – which enable them to do things that they wouldn't ordinarily have the ability to do – as in, load harmful programs on your PC.

You might stop and ask: if these are "known" security vulnerabilities hasn't Microsoft done anything about them?

In most cases, the answer is yes. Two challenges arise. One is that new security vulnerabilities appear frequently. The other is that even though Microsoft releases security fixes for known issues, the average person doesn't know about the fix -- or that they even need to think about things like security "fixing" their web browser.

In a way Microsoft's become a victim of its own success and popularity. Since so many people use their products – they've become an obvious target for hackers.

The Bottom Line: *by using a web browser other than IE, you will miss out on most of the current browser vulnerabilities.*

Currently [Firefox](#) is in the lead as the top alternative browser. The improvements over IE are numerous. Switching is easy – all your bookmarks are moved over automatically.

One thing to keep in mind, if you switch browsers you'll still need to keep IE around. It's rare, but there are some websites that will only display correctly in IE. In time this will change, but for the time being that's how it is.

Tip If you use and enjoy Firefox – make sure to read this [blog entry](#) to learn about free enhancements for Firefox.

Step 7: Take the 60 Second Security Challenge

This brings us to the 7th and final step – it's also a quick, hands-on exercise.

What's the "60 second security challenge?"

It's a way to quickly and easily get an overall sense of how secure your computer is at this very moment, and it only takes about a minute.

Interested?

Sygate, a software company, has kindly provided free security scans. They are web-based scans that are run from their website.

There are two recommended scans to run – each take about 30 seconds (depending on the speed of your Internet connection, of course).

Start by going to the link below:

⇒ [Sygate Security Scan](#)

Run the "Quick Scan" and "Stealth Scan" (you'll notice these links on the left side of the Window). Both will run and display a report.

So, what are you looking for?

The screenshot shows a Mozilla Firefox browser window displaying the Sygate Security Scan results for the IP address 71.106.87.228. The scan results are as follows:

Port	Type	Status	Additional Information
1999	Trojan	BLOCKED	This port has not responded to any of our probes. It appears to be completely stealthed.
6776	Trojan	BLOCKED	This port has not responded to any of our probes. It appears to be completely stealthed.
7789	Trojan	BLOCKED	This port has not responded to any of our probes. It appears to be completely stealthed.
12345	Trojan	BLOCKED	This port has not responded to any of our probes. It appears to be completely stealthed.
31337	Trojan	BLOCKED	This port has not responded to any of our probes. It appears to be completely stealthed.
54320	Trojan	BLOCKED	This port has not responded to any of our probes. It appears to be completely stealthed.
54321	Trojan	BLOCKED	This port has not responded to any of our probes. It appears to be completely stealthed.

Results from scan of ICMP at TCP/IP address: 71.106.87.228

Protocol	Type	Status	Additional Information
ICMP	8	BLOCKED	An ICMP ping request is usually used to test Internet access. However, an attacker can use it to determine if your computer is available and what OS you are running. This gives him valuable information when he is determining what type of attack to use against you.

You have blocked all of our probes! We still recommend running this test both with and without Sygate Personal Firewall enabled... so turn it off and try the test again.

Sygate Security Scan displaying a fully "stealthed" computer.

You want every scanned item to be reported as "blocked," as shown in the screen shot above. This means that your computer is completely "stealthed" while on the Internet.

A completely stealthed computer is one of the best defenses you can employ on the Internet.

Hackers and/or automated programs looking for systems to compromise will not even know you exist. Essentially you'll be flying "under the radar."

Hey, I'm Not Stealthed ... What Does this Mean?

Just to be clear, if either scan reveals even a single open item – **you are not fully stealthed** – so, what exactly does this mean?

The most critical things it means are:

- ⇒ At this very moment your computer is exposing information about itself to the Internet.
- ⇒ You're vulnerable to discovery by automated hacker tools called "port scanners." Note: port scanners are freely available scanning programs.
- ⇒ You have potential "back-door" entry points into your computer which could be exploited, and these need to be closed.

The Next Step ...

Would you like to learn all the simple steps and information you need to thoroughly secure and protect your valuable PC and private information?

We've provided the "missing" information that your Internet Service Provider and computer vendor didn't warn you about ... **and it's absolutely critical for today's Internet ...**

Finally, "Securing Your Computer Made Easy"



As the title suggests, **this is not a guide for "techies"** – it's simple-to-follow, step-by-step information written in plain English to help "everyday" people.

7 Easy Steps for Instantly Improving Your Online Security

If you have a Windows PC, these are the steps required to **thoroughly** protect your **PC, personal files** and **online identity**.

Here's just a sampling of what you'll learn:

- How to achieve "**stealth mode**" on the Internet -- without "stealth mode," **you're an open target on the Internet**.
- Simple Windows settings that will **greatly increase** your level of security.
- Why using **Windows built-in firewall** may still leave you vulnerable.
- How to protect your privacy and security over **Email** and **Instant Messaging**.
- What to do when your Anti-Virus program finds Viruses it can't remove.
- "Set it and forget it" – how to make Windows **automatically** keep itself up-to-date with the latest security fixes.

Won't it be nice to go back to using and enjoying the Internet *knowing* that you're well-protected against Internet security threats?

Please don't put this off any longer.

Click below to download your copy right now.

⇒ [Securing Your Computer Made Easy](#)