

# Understanding **Internet Security**

What you need to protect yourself online.

# Understanding Internet Security

*What you need to protect yourself online.*

## Table of Contents

### **SECTION ONE—Internet Security: What it is and why you need it**

- You and your family are at risk of virtual attacks .....1
- Understanding how the Internet works and the security threats you face.....1
- What's a nuisance, what's a threat .....2
- Spyware: It's the new threat your anti-virus software won't find .....2

### **SECTION TWO—Protecting yourself from Internet threats**

- How to know if you have been a victim of an Internet attack.....3
- Step One: Find out what's already on your computer .....4
- Step Two: Get rid of the threats.....4
- Step Three: Build a protective wall around your computer.....4
- Step Four: Filter out the Internet junk.....5

### **SECTION THREE—Advanced Protection. Simple Solution.**

- Identifying the right Internet security solution for you .....6
- Evaluating your risks with the BP Security Analyzer™ .....6
- Eliminating the threats with BP Internet Security™ Spy Sweeper™ .....6
- Protecting your identity and personal data with  
the BP Internet Security™ firewall.....7
- Controlling Web content with BP Internet Security™  
Web-filtering .....7
- Bringing it all together with the BP Internet Security™  
control panel .....7
- Making security your top priority with BP Internet Security™ .....7

### **SECTION FOUR—Glossary of Internet Security Terms .....8**

### **SECTION FIVE—Frequently Asked Questions about BP Internet Security™ .....10**

# 1

## SECTION ONE—Internet Security: What it is, and why you need it.

### You and your family are at risk of virtual attacks.

A decade ago, the Internet was something only “techies” talked about. It was a new limitless source of information, with very few users. Today, the Internet has already become an essential part of our lives. It’s where we access our banking records, credit card statements, tax returns and other highly sensitive personal information. By the end of this decade, over 2 billion people will be connected to the Internet—that’s about half the world’s current population.

But with all the good things the Internet offers us, it also opens the door to serious, potentially devastating threats. Unlike corporate and government computer systems, few personal computers have any safeguards beyond basic virus protection. That means anytime you’re online, you are a potential target for online criminals and hackers. And if you have high-speed Internet access, your computer is online most of the time, making Internet criminals and hackers a 24-hour-a-day, year-round threat to you, your personal information, and your family.

### Understanding how the Internet works and the security threats you face.

When you access the Internet, your computer sends a message over the Web that uniquely identifies your computer and where it is located. This allows the information you’ve requested to be returned to you. Often, this requested information carries with it unwanted hidden software created by hackers and online criminals. This software installs itself on your computer and can either be just a nuisance or pose a more serious threat to you, your identity and sensitive financial information. Usually the nuisances are visible and easy to identify, while the more dangerous threats are typically invisible, silent, and difficult to detect until it’s too late. The key to a safe, enjoyable Internet experience is understanding the difference between what’s a threat and what isn’t.

### The numbers: Internet threats to your security are real.

- In 2002, more than 10 million people were victims of identity theft, costing the average victim more than \$1,000 and a year’s time to repair their credit.<sup>1</sup>
- More than 95% of Internet users have inadequate protection from online threats.<sup>2</sup>
- Over 90% of computer users have dangerous “spyware” lurking on their computers without their knowledge.<sup>3</sup>
- In 2002, nearly 20 million people had the skills to hack a computer.<sup>4</sup>
- In 2003, Internet-related identity theft more than tripled.<sup>5</sup>
- Today, a typical online PC is “scanned” by outside intruders twelve times every day.<sup>6</sup>

1 – Federal Trade Commission Report 09/03/03

2 – SummitWatch 11/03

3 – TechNewsWorld 3/19/04

4 – Information Warfare Task Force

5 – USA Today 10/23/03

6 – National Strategy to Secure Cyberspace 9/02

## What's a nuisance, what's a threat.

Cookies, pop-ups, and adware are tools that track your online behavior, and are used to promote various products. Many cookies are harmless online information gathering and tracking tools. The majority of adware consists of pop-up ads that are merely unsolicited nuisances. The problem is that hackers and online criminals are increasingly using cookies and adware to quietly sneak onto your computer and to access your personal information without your knowledge. This “spyware” watches and records everything you do online, leaving your passwords, private account information, and other personal and sensitive information vulnerable.

Once captured, this information can be sent back to online criminals for use in accessing your private information, stealing your identity, and your money. It can also be used to hijack your computer for illegal purposes. **Spyware finds its way to your computer through:**

- Web sites you browse on the Internet.
- Adware and pop-ups that load onto your computer.
- Results of your Internet searches.
- Unusual eCommerce sites you visit.
- Software you download onto your computer from the Internet.
- Weaknesses in the operating system software you're using.

## Spyware: It's the new threat your anti-virus software won't find.

If you're even a casual computer user, chances are you've heard about viruses and what they can do to your computer. Viruses are serious threats that attack your computer and data, and generally disrupt your life; but they aren't used to steal your sensitive personal information. Internet criminals create spyware to do this. They want you to believe that anti-virus software is all the protection you need. As important as it is to your security, anti-virus software can't detect or stop this newer, more sophisticated threat from entering your computer. Stopping spyware requires even greater protection.

### Spyware: The new virus.

Spyware represents a new, more dangerous threat than viruses. What makes spyware so destructive? It attacks you. Here's a side-by-side comparison:

#### Virus:

- Damages data
- Written by hackers
- Infection is obvious and can be detected with anti-virus software.
- Most computer users are sufficiently protected.
- The threat is decreasing.

#### Spyware:

- Steals sensitive private information.
- Written by professional online criminals.
- Infection is silent and cannot be detected with anti-virus software.
- Very few computer users are protected.
- The threat is increasing.

# 2

## SECTION TWO—Protecting yourself from Internet threats.

### How to know if you have been a victim of an Internet attack.

Chances are you are already a victim of an Internet attack and aren't even aware of it. The fact is, over 90 percent of Internet users have spyware lurking on their computers without their knowledge<sup>1</sup>. To protect yourself, you need to be able to identify the common symptoms associated with an Internet attack.

**Some symptoms you may presently be experiencing include:**

- **Increasing amounts of unsolicited email**—This increase in email is a result of personal information collected by cookie programs that is sent back to the cookie originator, and then sold to other online marketing organizations.
- **Unwanted pop-up advertising**—The software that causes pop-ups to appear on your computer is a form of spyware, and is loaded on your computer without your knowledge when you visit certain Web sites.
- **Browser homepage changes without your knowledge**—Certain Web sites will load cookies onto your computer that automatically change your homepage to their Web site. It is an annoyance that happens frequently to Internet users.
- **Your computer operates slower than it has in the past**—Spyware loaded onto your computer uses the same computer memory that is needed to run your more important software programs. This results in a competition for memory in your computer, causing all of your more critical software programs to run more slowly.

<sup>1</sup> TechNewsWorld 3/19/04

### Julian Green: How Trojan Horses can devastate a person's life.

Meet Julian Green. Originally published in the New York Times, Julian's story illustrates what can happen to an innocent victim of criminal computer hackers. After purchasing a computer for his family, Julian was arrested for having illegal pornography stored on it. After weeks in jail, Julian was released after it was determined that he was an unknowing victim of 11 Trojan Horses, a common form of spyware, secretly loaded onto his computer—some before he purchased it, others while he browsed the Internet. These Trojan Horses allowed pornographers to download the images on his computer and use it to “host” their illegal activities. Though he was cleared of all wrongdoing, Julian lost his home and custody of his daughter, and his good name suffered irreparable damage.

The following process, in conjunction with good, comprehensive anti-virus software will help you protect your family and your personal information from these and many other Internet threats.

### **Step One: Find out what's already on your computer.**

The first thing you need to do is to find out whether or not you have spyware or other threatening software on your computer. This requires a good, comprehensive Internet security analysis tool that completely scans your computer for hidden files that would pose a danger or compromise the security of your personal information. The right scanning software will identify Trojan Horses, system monitors, adware, cookies and other dangerous spyware threats and will also review the Web sites that have been visited by anyone using your computer and alert you to any inappropriate content found on them. After a scan has been completed you'll have a better idea of how secure your computer, personal information, and family actually are.

### **Step Two: Get rid of the threats.**

Once the threats found on your computer have been identified, it's important to eliminate them as soon as possible. Every minute you wait increases the chances of you becoming a victim of financial and identity theft. This step requires that you use a solid anti-spyware software program which can isolate and eliminate the cookies, adware, system monitors, Trojan Horses, and other dangerous spyware found on your computer. Correctly using the right anti-spyware software will leave your computer free of these dangerous threats.



### **Step Three: Build a protective wall around your computer.**

Once you've eliminated all the potentially dangerous programs and cookies from your computer, you'll want to stay threat-free by adding a crucial safeguard called a firewall.

A firewall's job is a lot like the thick walls of a castle. It provides a barrier between you and potential attackers trying to access your computer. It acts as a draw-bridge, allowing only communication you control to pass through the gates of your Internet connection. An effective firewall blocks outside intruders who try to access your computer without your permission, giving you the added assurance that your personal information is guarded and safe.

#### **Step Four: Filter out the Internet junk.**

No one cares more about the safety and protection of your family than you do. Operators of Web-based businesses that deal in inappropriate Web-content and pornography set out with the goal of getting as many sets of eyes viewing their Web sites as possible, regardless of whether they belong to adults or children. The only sure way to protect those you care about is to manage the content and use of your computer yourself.

The most effective and efficient way to gain total control of your computer content is to install a proven Web-filtering software program (also known as “parental control” software). Good Web-filtering software lets you decide what’s permitted onto your computer through your browser and what will be denied access. Web-filtering software gives you the extra peace of mind that your family is safe from the barrage of unwanted content and messages that exist online.



#### **Louise Williams: Internet thieves stole her good name & her good credit.**

It started about four years ago. Louise Williams, a Nu Skin employee, started receiving calls from credit agencies about missed payments on credit card accounts she’d never opened. It seems that a woman in Allentown, Pennsylvania had stolen her social security number and was using it to open a number of accounts. The fact that the woman lived in a different state caused Louise to believe her identity was stolen online. Due to the frequent calls she receives, Louise is now forced to daily carry a 6” briefcase containing all of her information to answer credit agency questions. The incident has cost Louise nearly \$2,000 and almost 500 hours of time just to deal with the constant, and ongoing, calls from creditors.

# 3

## SECTION THREE—Advanced Protection. Simple Solution.

### Identifying the right Internet security solution for you

Deciding on the right Internet security solution is confusing to most people. But it is a critical decision to ensure that you're fully protected. Besides the confusion of deciding which products are needed, is the difficulty of installing and using typical security software. That's why we created BP Internet Security™—the most advanced, yet simple-to-use solution available today for combating Internet security problems. It combines the industry's leading, award winning, Internet security technologies into one innovative product. **BP Internet Security™ offers you and your family protection from:**

- Criminals who would steal your identity and money by obtaining social security numbers, credit card accounts, and other financial and personal information online.
- Hackers who would use your PC for their own illegal purposes.
- Pop-up advertising and spyware that's not just annoying, but dangerous as well.
- Inappropriate web content encountered while online.

What's more, the BP Internet Security™ product control panel lets you easily manage all of the tools in BP Internet Security™ from one, easy-to-use location on your computer desktop. Regardless of your overall computer knowledge, this product is simple to use. Teamed with your anti-virus software, BP Internet Security™ rounds out a total security solution that will protect you and your family from online threats.

### Evaluating your risks with BP Security Analyzer™.

To identify your need for BP Internet Security™, Big Planet has provided an easy-to-use, yet powerful analysis tool, the BP Security Analyzer™. The BP Security Analyzer™ quickly identifies dangerous spyware, harmful Web site content, and other Internet security threats on your personal computer. It will then recommend the course of action you need to take to properly protect yourself. Using the BP Security Analyzer™ is the right first step to securing your Internet connection. It can also be used to help you recommend the BP Internet Security™ solution to your friends, relatives, and neighbors.



### Eliminating the threats with BP Internet Security™ Spy Sweeper™.

Once identified, all possible threats to your online security need to be eliminated. BP Internet Security™ Spy Sweeper™ will quarantine and eliminate the threatening spyware, annoying adware and cookies, and destructive Trojan Horses that are found on your computer. Once your computer's clean, you'll see results through improved computer performance and you will see a drop in the number of pop-ups that appear.

## Protecting your identity and personal data with the BP Internet Security™ firewall.

After removing the threats from your computer, BP Internet Security™ helps you secure it from future Internet attacks with its award-winning firewall. In fact, the firewall has already been set up to immediately begin protecting your computer after installation. BP Internet Security™ alerts you whenever someone tries to access your computer from the Internet. You'll have total online control, plus peace-of-mind knowing your BP Internet Security™ firewall is constantly protecting you.

## Controlling Web content with BP Internet Security™ Web-filtering.

After cleaning and securing your computer from dangerous online threats, the sophisticated Web-filtering tool in BP Internet Security™ lets you decide what type of content you will allow through your browser and onto your computer. BP Internet Security™ instantly reviews the content on the Web sites you visit against the filtering settings you select to determine if the Web site content is acceptable. This ensures that even when you aren't there, your family is protected from Web content you decide is inappropriate.



## Bringing it all together with the BP Internet Security™ control panel.

Bringing all of these award-winning technologies together is the BP Internet Security™ control panel—a tool that's as easy to use as it is to understand. The control panel is where you will manage each of the tools in BP Internet Security™—Spy Sweeper™, the firewall, and the Web-filtering tools. It's completely protected so that only those with the proper password can make changes to the settings. It was built so that anyone desiring to secure their computer can do so, regardless of their comfort with, or knowledge of technology.

## Making security your top priority with BP Internet Security™.

The clock's ticking. Every minute you spend unprotected on the Internet exposes you to threats that could literally erase your financial well being, compromise your family's safety, and lead to the loss of your identity. Now's the time to get the protection you need.

Partnering with the top names in security software, Big Planet has brought together the award-winning Internet security components that make up BP Internet Security™. The result is the best and easiest-to-use Internet security solution available—a solution that anyone can use. And, it's only available from Big Planet.

To see how BP Internet Security™ stacks up against its leading competitors in the Internet security industry, visit the BP Internet Security™ product page at [www.bigplanetusa.com](http://www.bigplanetusa.com).

# 4

## SECTION 4—Glossary of Internet Security Terms

**Adware**—A form of spyware. Displays the “pop-up” ads you’ve seen on your computer. Advertisers use it to generate online revenue and exposure. Adware installs components that gather personal information without informing you that it’s doing so.

**Broadband**—High-speed Internet connection typically offered by cable and phone companies. Without adequate Internet security, Broadband users are constantly at risk of online security threats because their computers are always connected to the Internet.

**Cookies**—Bits of information secretly stored on your computer allowing others to monitor your Internet activities. This spyware is often used to gather information on your Web-surfing habits to help companies create better marketing strategies. However, many send information to online criminals who would use it to harm you.

**Firewall**—Software that sets up a defense barrier around your computer so that hackers and online criminals cannot access the information on your computer.

**Hackers**—Individuals with computer and Internet skill levels sufficient enough to break security settings on personal computers and servers over the Internet. Some hackers do it for recreation, others for malicious intent.

**Identity Theft**—Occurs when a criminal obtains and uses another individual’s personal information (social security numbers, financial account information, etc.) to use his or her identity for illegal purposes. They then conduct fraudulent activities in the victim’s name.

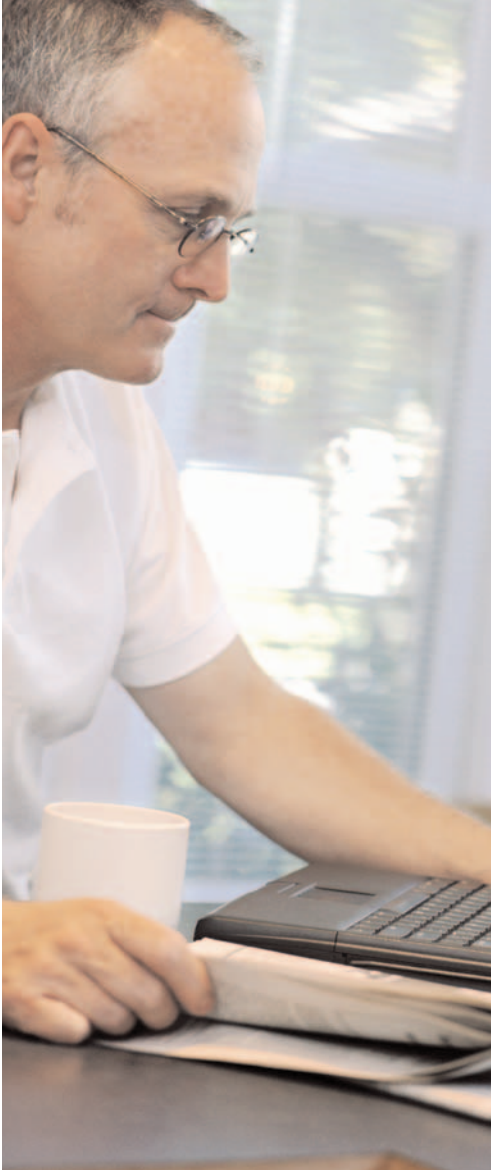
**ISP**—Internet Service Provider. An organization that offers Internet access to customers.

**Phishing**—A hoax where Internet criminals send out false emails in the name of a legitimate organization in order to trick victims into sending personal information back to be used in identity theft crimes.

**Spam**—Unsolicited promotional email.

**Spyware**—Dangerous software that collects information about your computer activities. It sends that information to others without your knowledge or permission. Once on your computer, spyware installs itself and starts working. It’s difficult to detect, and often impossible for average users to remove. Types of spyware include tracking cookies, adware, Trojan Horses, and system monitors.

**System Monitors**—Spyware that observes and captures keystrokes of virtually everything you do on your computer—including passwords, social security numbers, credit card numbers, emails and chat room dialogs. It also monitors the Web sites you’ve visited, and programs you’ve run. They usually run unnoticed, storing the information on your computer in a secret file to be retrieved later.



**Trojan Horses**—Spyware that is often disguised as harmless or even desirable programs, but is actually designed to cause loss or theft of computer data and to destroy computer systems. They usually arrive as email attachments or bundled with other software. Some give attackers unrestricted access to your computer anytime you're online, allowing file transfers, adding or deleting of files and programs, and taking control of your mouse and keyboard.

**Virus**—A software program written to disrupt computer systems and to destroy data—viruses are the most well known Internet security threat.

**Worms**—Similar to viruses but much more dangerous. They spread rapidly by accessing your email address book and automatically forwarding themselves to every address it contains. Current anti-virus software can't find worms once they've been loaded onto your system.

**Web filtering**—A software tool that allows computer users to determine which Web content they will allow onto your computer through their browser.

# 5

## SECTION 5— Frequently Asked Questions about BP Internet Security™

Listed below are some of the most frequently asked questions regarding BP Internet Security™. To review a more detailed list of questions please visit the BP Internet Security™ product website at [www.bigplanetusa.com](http://www.bigplanetusa.com).

**Q. *How technical do I have to be to use BP Internet Security™?***

A. You don't have to be technical at all. We have brought together award winning technologies and made them simple to use with our BP Internet Security™ control panel. It is a tool that is as easy to use as it is to understand. We developed BP Internet Security™ to be easy so that anyone with a basic understanding of how to turn on a computer can use this product.

**Q. *Who do I contact if I need help with my BP Internet Security™ software?***

A. It's easy. Big Planet technical support is available to all BP Internet Security™ customers. You can email a specific question, engage in a live chat, or access frequently asked questions from the technical support link on the BP Internet Security™ product page at [www.bigplanetusa.com](http://www.bigplanetusa.com).

Telephone support is also available at 1-800-487-1000 or 1-801-345-6617 during the hours of:

**Seven days-a-week**

5 a.m. to 11 p.m., PST

6 a.m. to midnight, MST

7 a.m. to 1 a.m., CST

8 a.m. to 2 a.m., EST

*Product support is currently available only in the United States*

**Q: *How does BP Internet Security™ compare to other products available on the Internet?***

A: There are hundreds of Internet security products available online. Many are of lower quality and won't adequately protect you from the evolving Internet threat. Some try to entice consumers with the promise of free downloads that will only work for 30 to 60 days. Once they expire, you're left unprotected. Through a unique combination of award-winning security software components, Big Planet offers you a complete Internet security solution. In fact, the technology that makes up BP Internet Security™ has received some of the highest ratings available in the Internet security industry.

**Q: *Why hasn't Big Planet included anti-virus software with BP Internet Security™?***

A: Anti-virus software is shipped with nearly all Windows-based PC systems. Because of this, Big Planet has focused on the areas of Internet security that have not been addressed for consumers. BP Internet Security™ will work seamlessly with the anti-virus software of your choice.

**Q: *How do the BP Security Analyzer™ and BP Internet Security™ work together?***

A: The BP Security Analyzer™ and BP Internet Security™ work hand-in-hand to secure your computer. The BP Security Analyzer™ is a powerful analysis tool that evaluates and assesses your computer's security risks. Within minutes, it identifies dangerous spyware, Trojan Horses, and other Internet security threats on your personal computer and then recommends the proper course of action to protect you. BP Internet Security™ is an advanced, easy-to-use Internet security software product that removes spyware and protects you from the latest Internet security threats, Internet fraud, objectionable web site content, and much more. BP Internet Security™ includes spy sweeping technology, the industry's top-rated firewall, and comprehensive Web-filtering tools.

**Q: *If I have more than one computer in my home, can I use BP Internet Security™ on all of them?***

A: Yes, however you must purchase a separate license for each computer on which you want to use BP Internet Security™.

**Q: *Will BP Internet Security™ work on computers attached to a network?***

A: Yes, BP Internet Security™ works very well on individual computers attached to a network. However, none of the other computers on the network will be protected.

**Q. *How do I know when a new version of BP Internet Security™ is available?***

A. BP Internet Security™ has a version update mechanism built right into the application. When a new version is available, you will be prompted with an “upgrade” dialogue box. Simply select the “Upgrade Now” button and you'll automatically receive the latest version of BP Internet Security™.

**Q. *What are the system requirements for BP Internet Security™?***

A. Windows 98SE/2000/XP  
333 MHz Pentium II Processor  
25 MB of available hard disk space  
48 MB RAM (98SE)  
64 MB RAM (2000)  
128 MB RAM (XP)  
Microsoft IE 5.5 and higher

**To learn more about the features and benefits of BP Internet Security™, please review the online tutorial and help options from the BP Internet Security™ product control panel.**



## **BP** Internet Security

Advanced Protection.  
Simple Solution.