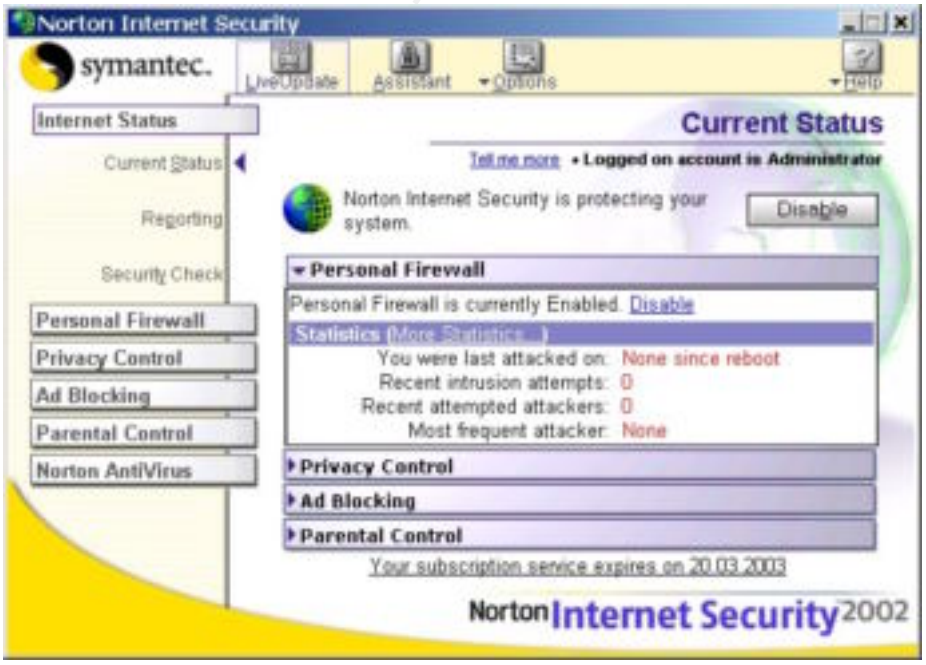
Global Information Assurance Certification Paper

Norton Internet Security 2002
Personal Firewall, Privacy Control, Ad blocking, Parental Control and AntiVirus
For Win98/Me, Win NT 4.0 WS, Win 2000 Pro, Win XP Home/XP Pro

GSEC Practical Version 1.3
Anton Bojanec
April 08, 2002

Abstract

Internet security is becoming an essential tool not only for doing business in the 21st century, but also for home users who are facing with more and more security challenges. These challenges are ranging from non harmful snooping, more or less harmful viruses and worms , to hackers trying to gain access to home PCs. While earlier vectors of delivering harmful content to a home user, such as physical access and file sharing via diskettes or CDs, are still a concern, the primary vectors for the introduction of harmful cont ent into home computers have now shifted. Today, the two primary vectors for the delivery of harmful content to home computers are: Internet access and email. This is where Norton Internet Security 2002 comes in. NIS 2002 is a complete integration of powerful components, which gives you a comprehensive protection against all sorts of Internet threats.



Product overview

NIS 2002 includes five main components that work together to protect your personal computer from Internet and email threats:

- Norton Personal Firewall - prevents unauthorized access to your computer when you are on the Internet
- Norton Privacy Control – protects your personal information
- Norton Ad Blocking – blocks Internet advertisements to speed up your Internet browsing
- Norton Parental Control – protects your family from inappropriate Internet content
- Norton AntiVirus – provides comprehensive virus protection, detection and elimination

NIS 2002 requirements are:

	Win 98/Me	Win NT 4.0 WS	Win 2000 Pro	Win XP Home/Pro
Processor	Pentium 150 MHz			Pentium 300 MHz
RAM	32 RAM	64 RAM		128 RAM
Disk space	60 MB without Parental Control installed or 90 MB with Parental Control installed			
Other	/	SP 6a or higher	/	/

You must also have Internet Explorer 4.01 Service Pack 1 or higher, CD -ROM or DVD-ROM and Microsoft Windows Internet support on your computer.

Steps to be taken before the installation:

- If you have any previous versions of Norton Internet Security or any other anti-virus software on your computer, you must uninstall them before installing NIS 2002.
- If you are using Win XP, disable the XP firewall.

Steps to be taken after the installation:

- Use LiveUpdate feature of NIS 2002 and get the latest program and virus definition updates from Symantec Web page.

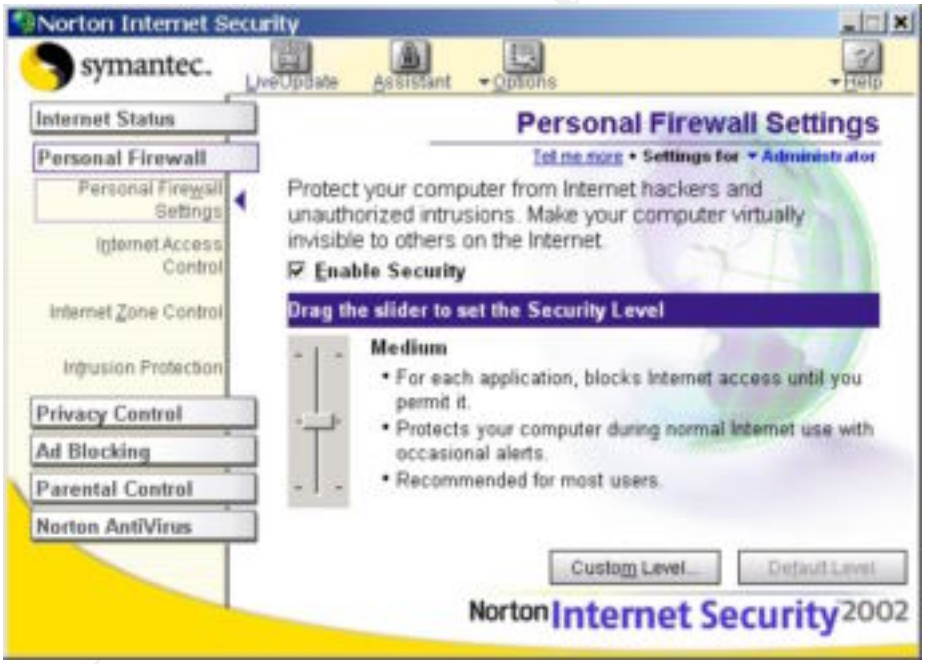
Personal Firewall

Norton Personal Firewall protects your computer from unauthorized access attempts. It protects your communications in both ways: it blocks attacks from other computers from Internet and controls Internet access for application on your computer.

The firewall provides four types of settings:

- Personal Firewall settings provide an overall Security Level setting that makes appropriate adjustments throughout the program
- Internet Access Control set access rules for the applications on your computer
- Internet Zone Control lets you access trusted computers and completely block restricted computers
- Intrusion Protection monitors hackers attempts to attack your computer and blocks computers that attack you from further access

NOTE: A very useful thing to do first is to make a scan for Internet-enabled applications. NIS 2002 scans your computer for applications that it recognizes and then lets you choose appropriate settings for each of them.



Security level

With the Security level option you can select the level of protection throughout Norton Personal Firewall. You set the settings for firewall, Java applets, ActiveX control and whether unused ports respond to access attempts.

	HIGH FW blocks everything, until allowed	MEDIUM FW blocks everything, until allowed	MINIMAL FW blocks only connections to Trojans
ActiveX	Prompts you each time	Can run	Can run

Java	Prompts you each time	Can run	Can run
Ports	Stealth appearance	Stealth appearance	Unused ports respond

The default setting is Medium, which is good balance b etween security benefits and issues of convenience and performance. In case this preset security settings doesn't match your needs you can change the settings for Firewall, Java, ActiveX and unused ports individual. Also you can choose whether you enable a ccess control alerts and alerts when unused ports are accessed.

Internet Access control

Here you can control how Internet -enabled applications on your computer access the Internet. You can do that with four additional options:

- **System-wide settings**: Here you can set the firewall rules that apply to the entire system. System -wide settings provide a series of rules that the firewall uses to allow or block various activities. You can add, change or delete any of the rules, but you **should have a good understanding what you are doing**. In every rule you can define action (permit, block, monitor), connections to permit (to other, from other or to and from other computers), computers to which the rule applies (any, specific computers and adapters - if you have more then one adapter), communications to permit (what protocol and port), type of tracking (log, notify with Alert tracker message or create security alert) and every rule has its description. The rules are applied in top to bottom order.
- **Trojan settings**: Provides protection for a variety of remote access Trojan horses starting from Back Orifice 2000 to QaZ. Every rule has the same parameters as the rules in system -wide settings and they are applied in top to bottom order, too. Every time you connect to LiveUpdate, the list of Trojan rules is being checked and new threats are added to the list.
- **Application scan**: Scans your machine for Internet -enabled applications that it recognizes and then lets you choose settings for each application. This is probably the qui ckest way to set up Internet access control for all your applications. For every application you can decide what kind of access do you allow (automatic configuration, permit, block or customize access) and to which group this application belongs (general, chat, …, web browser, user category or multiple).
- **Automatic Internet Access Control**: If this option is enabled then firewall automatically creates new rule for low -risk applications that it recognizes the first time that they are run. New rules will only b e created for known applications that have been identified as posing little risk to your computer.

Internet Zone Control

In the Internet Zone Control window you can specify computers that you trust and computers that you don't and want to restrict them fr om accessing your computer at all. Trusted computers have unlimited access to your computer, restricted computers have none.

You can place the computers in one of two zones:

- **Trusted zone**: Computers in a trusted zone have as much access to your computer as they would have if NIS 2002 would not be installed on your computer. Typically, if you have computers on your local network you should put them in a Trusted zone
- **Restricted zone**: Computers in a restricted zone are prevented from accessing your computer at all. You can have no interaction with the computers in a restricted zone. Typically, if some computers have attacked you in the past, you should put them in a Restricted zone.

You can put computers in zones individually (by IP or name), using an IP range or using a network address.

Intrusion Protection

Intrusion Protection part of NIS 2002 constantly monitors Internet communications, looking for patterns of communications that are typical of a hacker attack. For example, if a computer tries to connect to a series of ports on your computer, Intrusion Protection recognizes this as a port scan, which is a common method of probing your computer before the actual attack.
Intrusion Protection also detects attempts to connect to ports used by known remote-access Trojan horse programs. NIS 2002 is constantly upgrading its list of Trojan horse programs via its LiveUpdate feature.

When the program detects the probe or actual attack, it displays a warning and blocks all communications from the attacking computer for 30 minutes. This automatic blocking of communications is called AutoBlock. AutoBlock stops all communication from the remote computer for 30 minutes, but it does not stop you from communicating with the attacking computer.
Computers in the Trusted and Rest ricted zones are not subject to AutoBlock. These are two special groups of computers which means that computers in the Trusted zone are never blocked, while computers in the Restricted zone are permanently blocked.

Some normal Internet activities will be repeatedly recognized by Norton Personal Firewall as an attack. To prevent normal activities from interrupting your Internet use, you can exclude certain computers from being blocked by AutoBlock.

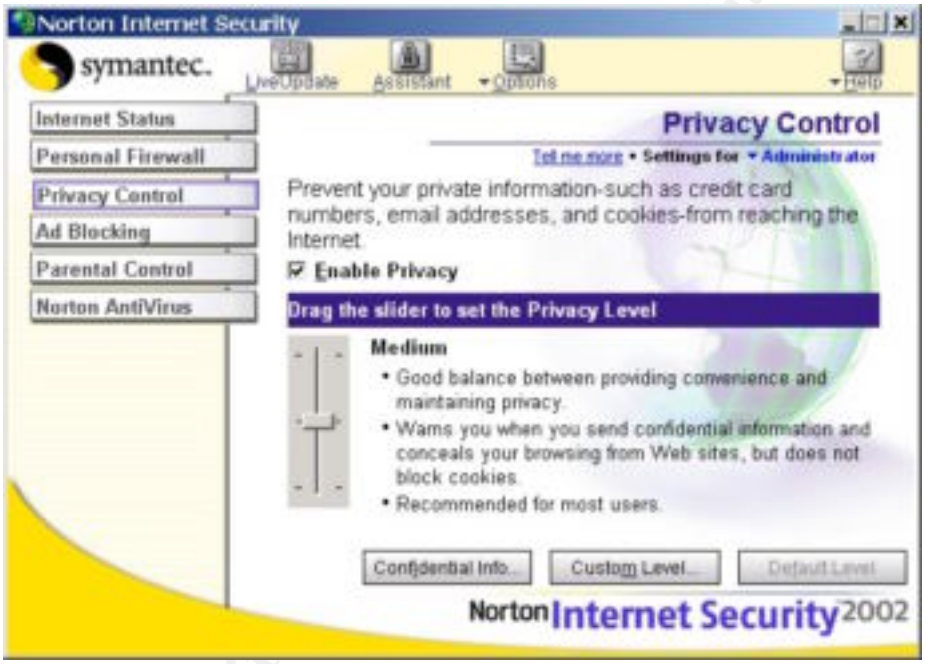
In the Intrusion Protection window you can see a list of c urrently blocked computers. You can unblock single computers, unblock all blocked computers, or even exclude computers from being blocked by AutoBlock if you are sure that traffic coming from them is legitimate, although NIS 2002 constantly displays warnin gs to you.

Privacy Control

Privacy Control ensures that you don't send private information such as credit card numbers over the Internet unless they are encrypted, or you specifically allow it. In the Privacy Control window you can view, modify, and en able Internet privacy settings which includes: personal confidential information,

cookies, addresses of the last visited Web sites and the email addresses used with the browser.
Cookies are small file that your browser saves on your computer and can be used to track your Internet usage. While most sites use cookies to remember the choices you have made on that site, some sites use cookies to track your browsing habits.

In order to NIS 2002 knows what your confidential data are you must first define them. All the confidential data is then stored in a single base and any confidential information you entered can be seen by users which have adult or supervisor rights.



After you defined your personal confidential information you can then use Privacy Level slider to set one of the following predefined Privacy Levels:

- **High:** NIS 2002 blocks all confidential information from being sent to nonsecured Web sites. You are prompted each time a cookie is sent to a Web page and browser privacy is enabled in order to prevent Web sites from retrieving the addresses of the last visited Web sites or the email addresses used within the browser.
- **Medium:** NIS 2002 prompts you each time confidential information is being sent to nonsecured Web sites – only admin account can sen d confidential information. Cookies are sent to a Web page without asking and browser privacy is enabled in order to prevent Web sites from retrieving the addresses of the last visited Web sites or the email addresses used with the browser.
- **Minimal:** NIS 2002 does not monitor confidential information sent to Web sites. Cookies are not blocked but browser privacy is still enabled

in order to prevent Web sites from retrieving the addresses of the last visited Web sites or the email addresses used with the brow ser.

The default setting is Medium what provides a good balance between security benefits and possible issues of convenience.
In case this preset security settings doesn't match your needs you can change the settings for confidential information, cookie blocking, and browser privacy individual. Also you can choose whether you enable secure connections (https) or not.

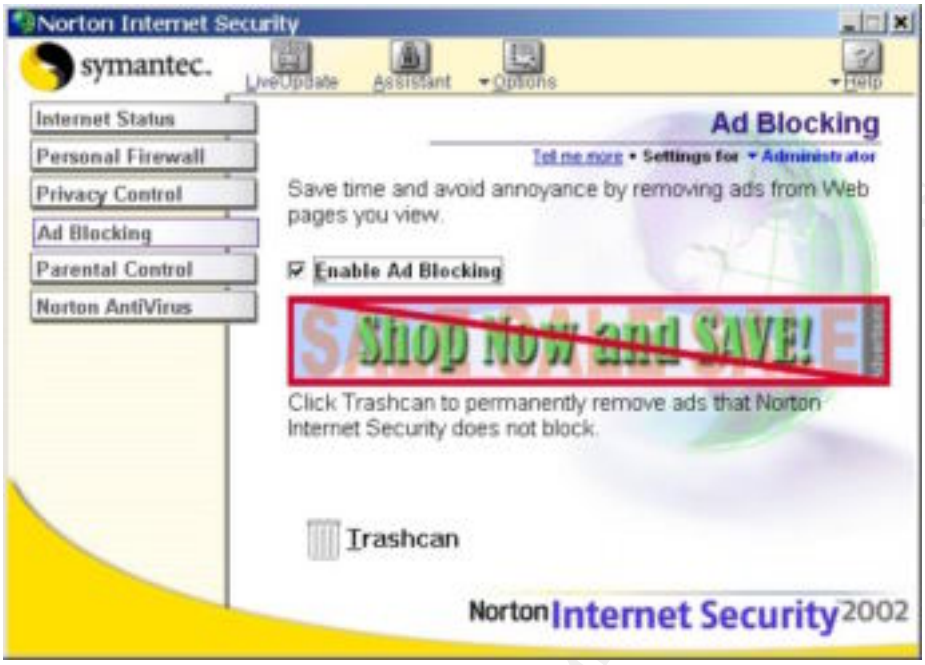
Because personal information is blocked exactly the way that you enter it into the program, it is better to enter only partial numbers or p arts of strings. For example, your Master card number could be typed as 1234 -5678-9012-3456, but it could also be entered without dashes (1234567890123456) or with spaces (1234 5678 9012 3456), or even more likely in four separate boxes. One common aspect of these formats is that the last four digits (3456) are always together. Thus, you can have better protection by protecting just the last four digits than you have by protecting the entire number.

Entering partial information has two advantages. First, you are not entering your complete credit card number where someone might find it. Second, it lets the program block your private information on sites that use multiple boxes for entering data.

NOTE: The program blocks confidential data sent to Web sites by means of HTTP only. It does not block data sent out by secure protocol (HTTPS) or through applications that use other protocols (email, chat programs, news readers, and so on).

Ad Blocking

Ad Blocking feature of NIS 2002 blocks Internet advertisement s and common graphics from downloading and by that helps you reduce the amount of time it takes to download a Web page. This feature applies only to banner ads within a Web page - ads built into the Web interface cannot be blocked.



NIS 2002 searches for the address of the ads being blocked as your browser downloads the Web page. It uses two lists to scan the Web pages as they are downloaded:

- **Default list**: This list of ads NIS 2002 blocks automatically and is constantly updated via LiveUpdate.
- **User custom list**: You create this list interactively as you are blocking ads. You can drag, or cut and paste, the graphic from the web site into the NIS 2002 ad Trashcan.

If NIS 2002 finds any addresses that match the list of ads to block, it removes the ad so that it does not appear in your browser. It leaves the rest of the Web page intact so that you can view the page without the advertisements.

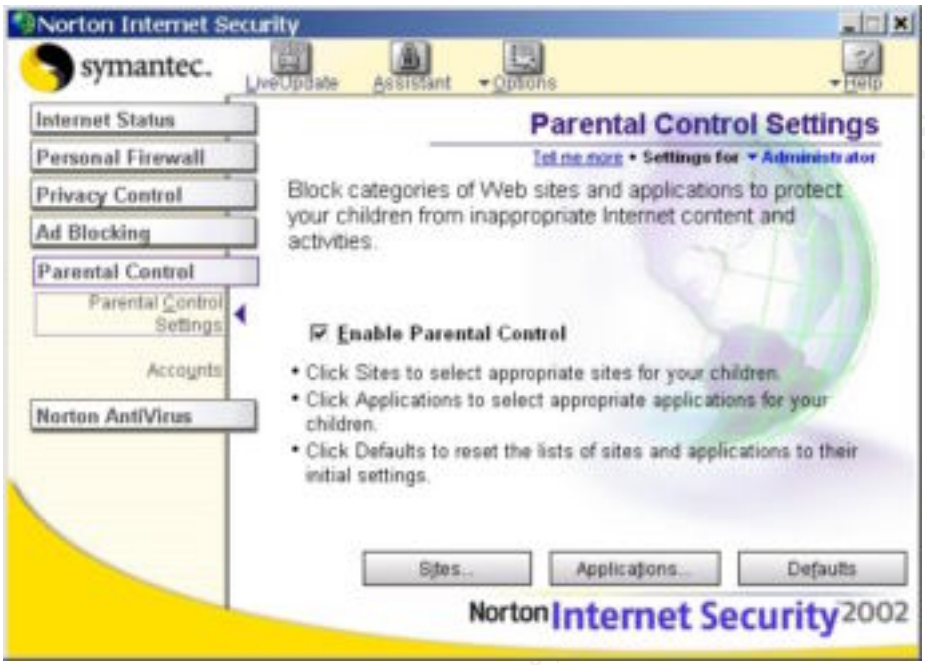
Parental Control

With the help of the Parental Control window, you can create a safer, more child-friendly Internet environment for your family members. NIS 2002 uses accounts to control access to Internet. An account stores the type of Internet access allowed for the users assigned to the account.

You can use Windows accounts (recommended) or you can create new on es, which are specific for NIS 2002. During the installation NIS 2002 creates Supervisor account and with this account you can change any of the settings in NIS 2002 and create additional accounts.

When no account is active, NIS 2002 uses the restricted se ttings of Not Logged In, which shuts down all Internet access.

By default, children's accounts do not block any Internet applications but they do restrict access to certain categories of Web sites.

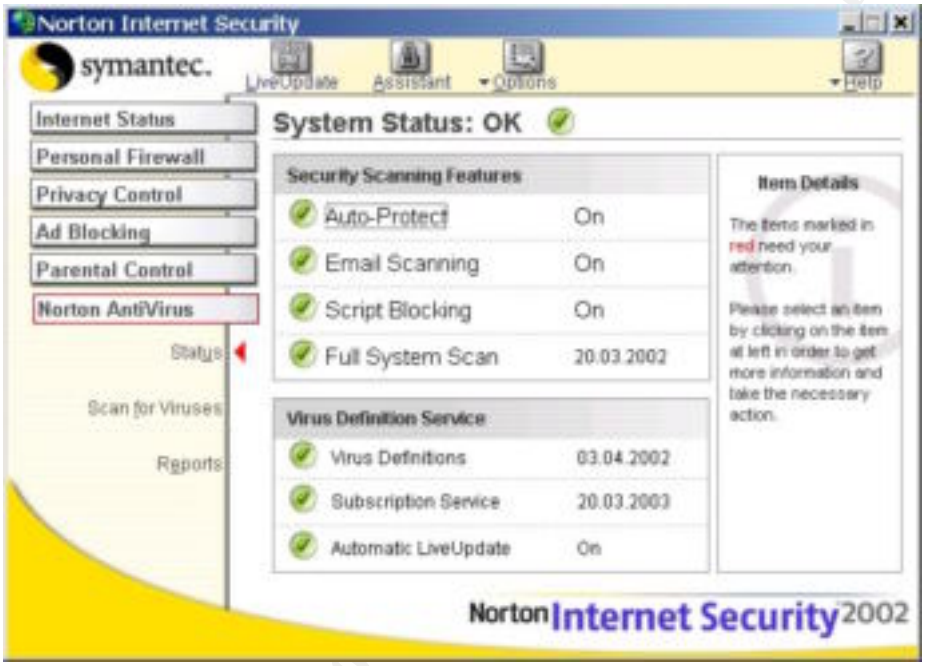


The controls in Parental Control window include:

- **Sites**: NIS 2002 lets you prevent family members from visiting Web sites with inappropriate or undesirable content. The basis of this feature is categorized list of Web sites that is created and maintained by Symantec and is constantly updated via NIS 2002 Li veUpdate option. This list includes more then 30 categories ranging from Adult Humour to Weapons. You can enforce parental control for each individual in your household in two ways: you can specify permitted sites or you can specify blocked sites. When you specify permitted sites you must build list of sites you specifically permit. On the other hand, if you choose to specify blocked sites you have a list of prohibited web sites categories already defined. You can ad specific sites to block them too, or you can even specify web page exceptions, which you allow to access.
- **Applications**: The basis of this feature is categorized list of internet - based applications that is created and maintained by Symantec and is constantly updated via NIS 2002 LiveUpdate optio n. This list includes more then 10 categories ranging from General to Web browser. NIS 2002 doesn't prevent restricted applications from running; it just prevents them from communicating over the Internet. **Note**: The Personal Firewall must be set to High to restrict the use of selected Internet-based applications.

Norton AntiVirus

Norton AntiVirus part of NIS 2002 is responsible for comprehensive virus protection, detection and elimination. It constantly searches and tries to repair infected files and by doing that keeps your data safe and secure. You can check the status of most Norton AntiVirus settings in the Status pane of the Norton AntiVirus main window. When nothing is red then the system should be reasonable protected.



Anti virus products depends heavily on current information to protect you from newly discovered threats. Norton AntiVirus has LiveUpdate feature, which downloads program updates and latest protection updates from Symantec Web site to your computer. You can manually start Live Update or you can set LiveUpdate to automatically check for new updates.

The default settings for Norton AntiVirus provide good virus protection, but in order to optimize your system performance or to simple disable the options you don't want you can customize every detail of Norton AntiVirus performance by clicking button Options. All the settings are organized into three main categories:

- System
- Internet
- Other

System options
The System options are those that determine what gets scanned, what the scan is looking for and what happens when a virus or virus -like activity is discovered.
In the System options you have following options:

- **Auto-Protect**: It allows you to customize the automatic protection feature in Norton AntiVirus. You can set Auto -Protect to starts every time you start your computer, what it looks for while monitoring the computer and what to do if it finds something. Auto -Protect has two additional subcategories: **Bloodhound** and **Advanced**. Bloodhound is scanning technology that dramatically i ncreases your virus protection against new and unknown viruses. It analyzes the program logic for virus-like behavior and monitors yours system activity for behaviors that viruses typically perform. Advanced options determine what activities to monitor whe n using floppy disk.
- **Script Blocking**: This option enables you to block scripts and to set what Norton AntiVirus does if it finds a malicious script.
- **Manual Scan**: This option enables you to determine which file types to scan, what to scan in addition to fi les and what to do if a virus is found. Manual scan option also has subcategory Bloodhound which you can enable or disable during the manual scans.
- **Exclusion**: The Exclusion option allows you to exclude files from being checked for viruses. You can exclude drives, folders, single file or groups of files.

Internet options
Internet options are those that determine what happens when your computer is connected to the Internet.
In the Internet options you have:

- **Email options**: The Email Protection options allow y ou to enable email scanning and define how Norton AntiVirus should behave while scanning email. You can choose to scan incoming emails, outgoing emails or both. Scanning incoming emails protects you from viruses sent by others while scanning outgoing email s prevents your from transmitting viruses to others.
- **LiveUpdate**: LiveUpdate option enables you to define how updates to NIS 2002 should be applied. If you enable automatic LiveUpdate then LiveUpdate automatically checks for updated virus definitions every four hours when you are connected to the Internet. **NOTE**: Automatic LiveUpdate checks and retrieves virus definitions only. To get program updates, you must run LiveUpdate manually.

Other options
Other options are those that determine a ctivity log settings and various miscellaneous settings.

- **Activity log**: The activity log records various Norton AntiVirus activities, which you chose from the list. You can also limit the size of the activity log. When the specified size is reached, each new entry in the log deletes the oldest logged entry.

- **Miscellaneous**: You have 4 options to set: what to do when repairing files (backup the file in Quarantine before attempting to repair?), how to keep Microsoft office documents protected (Norton AntiVirus scan Microsoft Office files when they are opened? - this option requires Microsoft Office 2000 or Office XP), what to do when virus protection is out of date (should Norton AntiVirus notify you when your virus definitions are more than two weeks old?) and what to do at system startup (which files to scan when your computer starts? – this option is available on Win98 and Win98Me operating systems only).

How to check your Norton Internet Security 2002 settings??

After all the hard work you put into the configuration of your NIS 2002 software, you want to know if you are safe. How?

Well, you have multiple options to do that:

- In your NIS 2002 you have Security check window, which enables you to test your computer's vulnerability to security intrusions. With the click on the link you are connected to the Symantec Security Check web page where your computer is then scanned for:
  - Network vulnerability scan
  - NETBIOS availability scan
  - Active Trojan horse scan
  - AntiVirus product scan
  - AntiVirus definition scan
  - Browser privacy scan
- Another option to probe your ports is by using two options from the Web site **www.grc.com**:
  - "Test my shields" attempts to contact hidden Internet server within your computer, attempts to contact port 139 and atte mpts to contact NetBIOS.
  - "Probe my ports" attempts to establish standard TCP Internet connections with a group of standard, well known, 13 service ports on your computer. If all of the probed ports report stealth status then your computer doesn't exist to scanners on the Internet.
- On the same Web site you have another utility, which is called LeakTest. Its purpose is to test your firewall configuration. Downlo ad it and run on your computer.

References:

Symantec, Inc. "Norton Internet Security 2002, User's guide":

Symantec, Inc. "Norton Internet Security 2002, Help files":

Symantec, Inc. "Product page":
http://www.symantec.com/sabu/nis/nis_pe/

Symantec, Inc. "Product service & support page":
http://www.symantec.com/techsupp/nis/nis_2002_tasks.html

Symantec, Inc. "Syman tec security check service page"
http://security1.norton.com/ssc/home.asp?j=1&langid=us&venid=symnis&plfid=22

Gibson research corporation, Steve Gibson
"NanoProbe Technology Internet Security Testing for Windows Users"
https://grc.com/x/ne.dll?bh0bkyd2

Gibson research corporation, Steve Gibson
"Internet Connection Security for Windows Users"
http://grc.com/lt/leaktest.htm

TechTV, "Review: Norton Internet Security 2002"
http://www.techtv.com/news/story/0,24195,3350378,00.html

CNet, "CNet review: Norton Internet Security 2002"
http://www.cnet.com/software/0-352108-1205-844863.html?tag=st.sw.352108-1204-6844863.dir-rev.352108-1205-6844863

InfoSecurityMag, "Test center: Norton Internet Security 2001"
http://www.infosecuritymag.com/articles/april01/departments_products1.shtml.