



INFORMATION TECHNOLOGY SUPPORT SERVICE

Level - I

LEARNING GUIDE 34

Unit of Competence: Protect Application or System Software

Module Title: Protecting Application or System Software

LG Code: ICT ITS1 M09 LO2 – LG34

TTLM Code: ICT ITS1 TTLM 1019v1

**LO 2: Detect and Remove
Destructive Software**



Instruction Sheet	Learning Guide 34
--------------------------	--------------------------

This learning guide is developed to provide you the necessary information regarding the following content coverage and topics –

- Common types of destructive software
- Selecting and Installing Virus Protection Software
- Advanced systems of protection
- Installing software updates
- Configuring software security settings

This guide will also assist you to attain the learning outcome stated in the cover page. Specifically, upon completion of this Learning Guide, you will be able to –

- Defining and identifying common types of destructive software
- Selecting and installing virus protection compatible with the operating system
- Describing advanced systems of protection
- Installing software updates on a regular basis
- Configuring software security settings
- Running and/or scheduling virus protection software on a regular basis
- Reporting detected destructive software
- Removing destructive software

Learning Instructions:

1. Read the specific objectives of this Learning Guide.
2. Follow the instructions described below 3 to 6.
3. Read the information written in the information “Sheet 1, Sheet 2, Sheet 3, Sheet 4 and Sheet 5” in page 3, 14, 26, 30 and 35 respectively.
4. Accomplish the “Self-check 1, Self-check 2 and Self-check 3” in page 12, 24, 28, 33 and 37 respectively
5. If you earned a satisfactory evaluation from the “Self-check” proceed to “Operation Sheet 1, Operation Sheet 2 and Operation Sheet 3” in page 39
6. Do the “LAP test” in page



1.1. Destructive Software

Destructive software is referred to as **malware** (malicious software) and the term includes **viruses, worms, logic bombs, rootkits, Trojan horses, adware, keystroke loggers** and **spyware**. **Malware** is software designed to infiltrate a computer system without the owner's informed consent; hostile, intrusive, or annoying software.

Data-stealing malware is a threat that divests victims of personal or proprietary information with the intent of monetizing stolen data through direct use or distribution. This type of malware includes **key loggers, screen scrapers, spyware, adware, backdoors** and **bots**. **Malware's** most common pathway from criminals or malicious developers to users is through the Internet: primarily by email and the World Wide Web.

The target of malicious software can be a single computer and its operating system, a network or an application.

1.2. The Common Types of Destructive Software

The common types of destructive software are:

- **Virus**

A computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability.

- **Worm**

Write Once, Read Many (Write One, Read Multiple or WORM); a software program capable of reproducing itself that can spread from one computer to the next over a network; WORMs take advantage of automatic file sending and receiving features found on many computers; self-replicating Malware computer program;

- **Logic Bomb**

Set of instructions inserted into a program that are designed to execute (or 'explode') if a particular condition is satisfied; when exploded it may delete or corrupt data, or print a spurious message, or have other harmful effects; it could be triggered by a change in a file, by a particular input sequence to the program, or at a particular time or date.



- **Rootkit**

A type of malware that is designed to gain administrative-level control over a computer system without being detected

- **Trojan Horse**

A Trojan, as the name implies, secretly carries often-damaging software in the guise of an innocuous program, often in an email attachment.

- **Adware**

Adware is software that loads itself onto a computer and tracks the user's browsing habits or pops up advertisements while the computer is in use. Adware and spyware disrupt your privacy and can slow down your computer as well as contaminate your operating system or data files

- **KeyLogger**

The practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored

- **Spyware**

Software that obtains information from a user's computer without the user's knowledge or consent

- **Screen Scrapers**

To extract data from (a source such as a webpage) by picking it out from among the human-readable content

- **Backdoor**

An undocumented way to get access to a computer system or the data it contains

- **Bots**

Also known as Crawlers or Spiders, bots are search engine programs that perform automated tasks on the internet – they follow links, and read through the pages in order to index the site in a search engine.

Greyware (grayware): a general term sometimes used as a classification for applications that behave in a manner that is annoying or undesirable but less serious or troublesome than malware; greyware encompasses spyware, adware, dialers, joke programs, remote access tools, and any other unwelcome files and programs apart from viruses that are designed to harm the performance of computers on your network.



1.3. Virus Origin, History and Evolution

1.3.1. Virus Origins

Computer viruses are called viruses because they share some of the traits of biological viruses. A computer virus passes from computer to computer like a biological virus passes from person to person.

Unlike a cell, a virus has no way to reproduce by itself. Instead, a biological virus must inject its DNA into a cell. The viral DNA then uses the cell's existing machinery to reproduce itself. In some cases, the cell fills with new viral particles until it bursts, releasing the virus. In other cases, the new virus particles bud off the cell one at a time, and the cell remains alive.

A computer virus shares some of these traits. A computer virus must **piggyback** on top of some other program or document in order to launch. Once it is running, it can infect other programs or documents. Obviously, the analogy between computer and biological viruses stretches things a bit, but there are enough similarities that the name sticks.

People write computer viruses. A person has to write the code, test it to make sure it spreads properly and then release it. A person also designs the virus's attack phase, whether it's a silly message or the destruction of a hard disk. Why do they do it?

There are at least three reasons. The first is the same psychology that drives vandals and arsonists. Why would someone want to break a window on someone's car, paint signs on buildings or burn down a beautiful forest? For some people, that seems to be a thrill. If that sort of person knows computer programming, then he or she may funnel energy into the creation of destructive viruses.

The second reason has to do with the thrill of watching things blow up. Some people have a fascination with things like explosions and car wrecks. When you were growing up, there might have been a kid in your neighborhood who learned how to make gunpowder. And that kid probably built bigger and bigger bombs until he either got bored or did some serious damage to himself. Creating a virus is a little like that -- it creates a bomb inside a computer, and the more computers that get infected the more "fun" the explosion.

The third reason involves bragging rights, or the thrill of doing it. Sort of like Mount Everest -- the mountain is there, so someone is compelled to climb it. If you are a certain type of programmer who sees a security hole that could be exploited, you might simply be compelled to exploit the hole yourself before someone else beats you to it.

Of course, most virus creators seem to miss the point that they cause real damage to real people with their creations. Destroying everything on a person's hard disk is real damage. Forcing a large company to waste thousands of hours



cleaning up after a virus is real damage. Even a silly message is real damage because someone has to waste time getting rid of it. For this reason, the legal system is getting much harsher in punishing the people who create viruses.

1.3.2. Virus History

Traditional computer viruses were first widely seen in the late 1980s, and they came about because of several factors. The first factor was the spread of personal computers (**PCs**). Prior to the 1980s, home computers were nearly non-existent or they were toys. Real computers were rare, and they were locked away for use by "experts." During the 1980s, real computers started to spread to businesses and homes because of the popularity of the IBM PC (released in 1982) and the Apple Macintosh (released in 1984). By the late 1980s, PCs were widespread in businesses, homes and college campuses.

The second factor was the use of computer **bulletin boards**. People could dial up a bulletin board with a modem and download programs of all types. Games were extremely popular, and so were simple word processors, spreadsheets and other productivity software. Bulletin boards led to the precursor of the virus known as the **Trojan horse**. A Trojan horse is a program with a cool-sounding name and description. So you download it. When you run the program, however, it does something uncool like erasing your disk. You think you are getting a neat game, but it wipes out your system. Trojan horses only hit a small number of people because they are quickly discovered, the infected programs are removed and word of the danger spreads among users.



Figure 1-1 Floppy disks were factors in the spread of computer viruses.

The third factor that led to the creation of viruses was the **floppy disk**. In the 1980s, programs were small, and you could fit the entire operating system, a few programs and some documents onto a floppy disk or two. Many computers did not have hard disks, so when you turned on your machine it would load the operating system and everything else from the floppy disk. Virus authors took advantage of this to create the first self-replicating programs.

Early viruses were pieces of code attached to a common program like a popular game or a popular word processor. A person might download an infected game from a bulletin board and run it. A virus like this is a small piece of code embedded in a larger, legitimate program. When the user runs the legitimate program, the virus loads itself into memory and looks around to see if it can find any other programs on the disk. If it can find one, it modifies the program to add



the virus's code into the program. Then the virus launches the "real program." The user really has no way to know that the virus ever ran. Unfortunately, the virus has now reproduced itself, so two programs are infected. The next time the user launches either of those programs, they infect other programs, and the cycle continues.

If one of the infected programs is given to another person on a floppy disk, or if it is uploaded to a bulletin board, then other programs get infected. This is how the virus spreads.

The spreading part is the **infection** phase of the virus. Viruses wouldn't be so violently despised if all they did was replicate themselves. Most viruses also have a destructive **attack** phase where they do damage. Some sort of trigger will activate the attack phase, and the virus will then do something -- anything from printing a silly message on the screen to erasing all of your data. The trigger might be a specific date, the number of times the virus has been replicated or something similar.

1.3.3. Virus Evolution

As virus creators became more sophisticated, they learned new tricks. One important trick was the ability to load viruses into memory so they could keep running in the background as long as the computer remained on. This gave viruses a much more effective way to replicate themselves. Another trick was the ability to infect the **boot sector** on floppy disks and hard disks. The boot sector is a small program that is the first part of the operating system that the computer loads. It contains a tiny program that tells the computer how to load the rest of the operating system. By putting its code in the boot sector, a virus can **guarantee it is executed**. It can load itself into memory immediately and run whenever the computer is on. Boot sector viruses can infect the boot sector of any floppy disk inserted in the machine, and on college campuses, where lots of people share machines, they could spread like wildfire.

In general, neither executable nor boot sector viruses are very threatening any longer. The first reason for the decline has been the huge size of today's programs. Nearly every program you buy today comes on a compact disc. Compact discs (CDs) cannot be modified, and that makes viral infection of a CD unlikely, unless the manufacturer permits a virus to be burned onto the CD during production. The programs are so big that the only easy way to move them around is to buy the CD. People certainly can't carry applications around on floppy disks like they did in the 1980s, when floppies full of programs were traded like baseball cards. Boot sector viruses have also declined because operating systems now protect the boot sector.

Infection from boot sector viruses and executable viruses is still possible. Even so, it is a lot harder, and these viruses don't spread nearly as quickly as they once did. Call it "shrinking habitat," if you want to use a biological analogy. The



environment of floppy disks, small programs and weak operating systems made these viruses possible in the 1980s, but that environmental niche has been largely eliminated by huge executables, unchangeable CDs and better operating system safeguards. E-mail viruses are probably the most familiar to you. We'll look at some in the next section.

- **E-mail Viruses**

Virus authors adapted to the changing computing environment by creating the **e-mail virus**. For example, the **Melissa virus** in March 1999 was spectacular. Melissa spread in Microsoft Word documents sent via e-mail, and it worked like this:

Someone created the virus as a Word document and uploaded it to an Internet newsgroup. Anyone who downloaded the document and opened it would trigger the virus. The virus would then send the document (and therefore itself) in an e-mail message to the first 50 people in the person's address book. The e-mail message contained a friendly note that included the person's name, so the recipient would open the document, thinking it was harmless. The virus would then create 50 new messages from the recipient's machine. At that rate, the Melissa virus quickly became the fastest-spreading virus anyone had seen at the time. As mentioned earlier, it forced a number of large companies to shut down their e-mail systems.

- **Worms**

A **worm** is a computer program that has the ability to copy itself from machine to machine. Worms use up computer time and network bandwidth when they replicate, and often carry payloads that do considerable damage. A worm called **Code Red** made huge headlines in 2001. Experts predicted that this worm could clog the Internet so effectively that things would completely grind to a halt.

A worm usually exploits some sort of **security hole** in a piece of software or the operating system. For example, the Slammer worm (which caused mayhem in January 2003) exploited a hole in Microsoft's SQL server. "Wired" magazine took a fascinating look inside Slammer's tiny (376 byte) program.

Worms normally move around and infect other machines through computer networks. Using a network, a worm can expand from a single copy incredibly quickly. The Code Red worm replicated itself more than 250,000 times in approximately nine hours on July 19, 2001 [Source: Rhodes].

The Code Red worm slowed down Internet traffic when it began to replicate itself, but not nearly as badly as predicted. Each copy of the worm scanned the Internet for Windows NT or Windows 2000 servers that did not have the Microsoft security patch installed. Each time it found an unsecured server, the worm copied itself to that server. The new copy then scanned for other



servers to infect. Depending on the number of unsecured servers, a worm could conceivably create hundreds of thousands of copies.

The Code Red worm had instructions to do three things:

- ✓ Replicate itself for the first 20 days of each month
- ✓ Replace Webpages on infected servers with a page featuring the message "Hacked by Chinese"
- ✓ Launch a concerted attack on the White House Web site in an attempt to overwhelm it

Upon successful infection, Code Red would wait for the appointed hour and connect to the www.whitehouse.gov domain. This attack would consist of the infected systems simultaneously sending 100 connections to port 80 of www.whitehouse.gov (198.137.240.91).

The U.S. government changed the IP address of www.whitehouse.gov to circumvent that particular threat from the worm and issued a general warning about the worm, advising users of Windows NT or Windows 2000 Web servers to make sure they installed the security patch. .

A worm called Storm, which showed up in 2007, immediately started making a name for itself. Storm uses social engineering techniques to trick users into loading the worm on their computers. So far, it's working -- experts believe between one million and 50 million computers have been infected [source: Schneier].

When the worm is launched, it opens a back door into the computer, adds the infected machine to a botnet and installs code that hides itself. The botnets are small peer-to-peer groups rather than a larger, more easily identified network. Experts think the people controlling Storm rent out their micro-botnets to deliver spam or adware, or for denial-of-service attacks on Web sites.

1.4. Types of Viruses

Viruses are split into different categories, depending on what they do. Here are a few categories of viruses:

- **Boot Sector Virus**

The Boot Sector of a PC is a part of your computer that gets accessed first when you turn it on. It tells Windows what to do and what to load. It's like a "Things To Do" list. The Boot Sector is also known as the Master Boot Record. A boot sector virus is designed to attack this, causing your PC to refuse to start at all!

- **File Virus**

A file virus, as its name suggests, attacks files on your computer. Also attacks entire programs, though.



- **Macro Virus**
These types of virus are written specifically to infect Microsoft Office documents (Word, Excel PowerPoint, etc.) A Word document can contain a Macro Virus. You usually need to open a document in a Microsoft Office application before the virus can do any harm.
- **Multipartite Virus**
A multipartite virus is designed to infect both the boot sector and files on your computer
- **Polymorphic Virus**
This type of virus alters their own code when they infect another computer. They do this to try and avoid detection by anti-virus programs.
- **Electronic Mail (Email) Virus**
Refers to the delivery mechanism rather than the infection target or behavior. Email can be used to transmit any of the above types of virus by copying and emailing itself to every address in the victim's email address book, usually within an email attachment. Each time a recipient opens the infected attachment, the virus harvests that victim's email address book and repeats its propagation process.

1.5. Virus Infection, Removal and Prevention

1.5.1. Virus Infection

The most common way that a virus gets on your computer is by an **email attachment**. If you open the attachment, and your anti-virus program doesn't detect it, then that is enough to infect your computer. Some people go so far as NOT opening attachments at all, but simply deleting the entire message as soon as it comes in. While this approach will greatly reduce your chances of becoming infected, it may offend those relatives of yours who have just sent you the latest pictures of little Johnny!

You can also get viruses by **downloading programs from the internet**. That great piece of freeware you spotted from an obscure site may not be so great after all. It could well be infecting your PC as the main program is installing.

If your PC is running any version of Windows, and it **hasn't got all the latest patches and updates**, then your computer will be attacked a few minutes after going on the internet! (Non Windows users can go into smug mode!)

Nowadays, they utilized the use of **removable storage devices** to spread viruses. The most common is the use of flash drive. Since removable drives like flash drive, CD/DVDs have the **autorun functionality**, *a simple command that enables the executable file to run automatically*, they exploited and altered it so it will automatically run the virus (normally with .exe, .bat, .vbs format) when you insert your flash drive or CD/DVDs.



Virus Infection Symptoms

Common symptoms of a virus-infected computer include

- Unusually slow running speeds
- Failure to respond to user input
- System crashes and constant system restarts that are triggered automatically.
- Individual applications also might stop working correctly,
- Disk drives might become inaccessible,
- Unusual error messages may pop up on the screen,
- Menus and dialog boxes can become distorted and peripherals like printers might stop responding.
- You can't access your disk drives
- Other symptoms to look out for are strange error messages, documents not printing correctly, and distorted menus and dialogue boxes.

Try not to panic if your computer is exhibiting one or two items on the list. Keep in mind that these types of hardware and software problems are not always caused by viruses, but infection is certainly a strong possibility that is worth investigating.

1.5.2. Removal of Viruses

The first step in removing computer is **installing any updates** that are available for your operating system; modern operating systems will automatically look for updates if they are connected to the Internet. If you do not already **have anti-virus software** on your computer, install and use the **anti-virus software** to do a complete scan of your computer. Since new computer viruses are constantly being created, set your anti-virus program to automatically check for updates regularly.

1.5.3. Prevention from Virus Infections

In order to prevent future computer infections:

- use an **Internet firewall**,
- check for operating system and anti-virus program updates,
- scan your computer regularly and exercise caution when handling email and Internet files.

A **firewall** is a program or piece of hardware that helps screen out viruses, worms and hackers which are attempting to interact with your computer via the Internet. On modern computers, firewalls come pre-installed and are turned on by default, so you probably already have one running in the background. When opening email attachments, don't assume they are safe just because they come from a friend or reliable source; the sender may have unknowingly forwarded an attachment that contains a virus.



Self-Check - 1	Written Test
-----------------------	---------------------

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

Part I: Say True or False

- _____ 1. Once the infected program has been run or installed the virus is activated and begins to spread itself to other programs on the current system.
- _____ 2. Adware and spyware not disrupt your privacy and can slow down your computer as well as contaminate your operating system or data files
- _____ 3. Virus authors are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer.
- _____ 4. Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software.
- _____ 5. Email Virus refers to the delivery mechanism rather than the infection target or behaviour.

Part II: Matching Column A with the Column B

Column A

- _____ 1. Logic Bomb
- _____ 2. Rootkit
- _____ 3. Adware
- _____ 4. KeyLogger
- _____ 5. Spyware
- _____ 6. Boot Sector Virus
- _____ 7. File Virus
- _____ 8. Macro Virus
- _____ 9. Multipartite Virus
- _____ 10. Polymorphic Virus

Column B

- A.** A type of virus alters their own code when they infect another computer.
- B.** A virus that is designed to infect both the boot sector and files on your computer
- C.** Types of virus that are written specifically to infect Microsoft Office documents (Word, Excel PowerPoint, etc.)
- D.** A virus that attacks files on your computer and also attacks entire programs.
- E.** A virus that is designed to attack a boot sector, causing your PC to refuse to start at all!
- F.** Software that obtains information from a user's computer without the user's knowledge or consent
- G.** The practice of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored
- H.** Software that loads itself onto a computer and tracks the user's browsing habits or pops up



Answer Sheet

Score = _____

Rating: _____

Name: _____

Date: _____

Part I: Say True or False

1. _____

2. _____

3. _____

4. _____

5. _____

Part II: Matching Column A with the Column B

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

7. _____

8. _____

9. _____

10. _____

Note: Satisfactory rating - 8 points

Unsatisfactory - below 8 points

You can ask your teacher for the copy of the correct answers.



2.1. Protection Software

We used to call everything a virus, however there are more precise names to further categorize **malware** – among them **virus**, **worm**, **Trojan**, **spyware**, **malware** and **adware**, to name a few.

Infection can have a devastating effect on the functioning of stand-alone machines and networks and can cause irretrievable damage to data and other resources. It is imperative to develop mechanisms to avoid infection. Detecting **malware** is a very sophisticated and well-defined process. Consequently, network administrators rely often rely on third party products to manage this process.

There is a variety of software packages available for both Single Device and Enterprise/Networked devices.

2.1.1. Single User

There are many kinds of protection software available for a single use device. Among them are

- Avast
- AVG
- Avira
- Bitdefender
- BullGuard
- Emsisoft
- ESET NOD32
- Fortinet
- F-Secure
- GData
- Kaspersky
- Kingsoft
- McAfee
- Microsoft Security Essentials
- Panda Cloud
- Qihoo 360
- Sophos
- ThreatTrack Vipre
- Trend Micro Titanium

Specialised software for removal such as Spybot Search & Destroy, Malwarebytes anti-malware and WinZip Malware Protector.

Other specialised programs that can block certain known IP addresses of hackers, unwanted advertising companies. One program that does this is PeerBlock. PeerBlock blocks "known bad" computers from accessing yours, and vice versa. Depending on the lists you have it set up to use, you can block governments, corporations, machines flagged for anti-peer-to-peer activities, even entire countries. The down side of this is that you will have to keep an eye on the program as it can block legitimate sites just because they have possibly been used for hacking attempts.

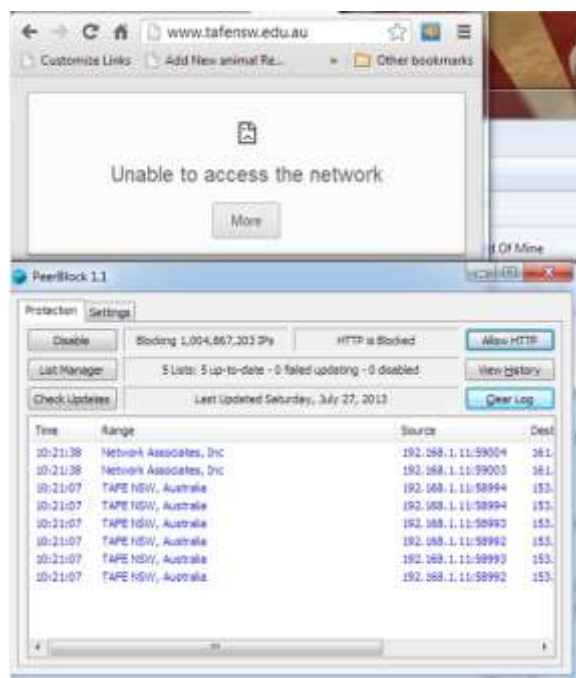


Figure 3-1: PeerBlock – What happens when blocking TAFE website

With Peerblock you can edit your lists and add or remove addresses from the lists so that you can still control which computers you can or cannot access.

2.1.2. Multi User/Enterprise

Even though small business antivirus software is usually priced on a per-user basis with a cost that is on par with individual-user products, it often gives business owners important additional features such as the ability to install and manage all installations from a central location. Some of the available products are:

- Bitdefender Small Business Pack
- Kaspersky Endpoint Security for Business
- F-Secure Small Business Suite
- Symantec Endpoint Protection
- G Data AntiVirus Business
- Webroot Secure Anywhere Business
- Vipre Business Premium
- avast! Endpoint Protection Suite
- Panda Security for Business
- Total Defense Threat Manage



2.2. Anti-Virus Software

Antivirus or **anti-virus software** is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spyware and adware. This page talks about the software used for the prevention and removal of such threats, rather than computer security implemented by software methods.

No matter how useful antivirus software can be, it can sometimes have drawbacks. Antivirus software can **impair** a computer's performance. Inexperienced users may also have trouble understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach. If the antivirus software employs heuristic detection, success depends on achieving the right balance between false positives and false negatives. **False positives** can be as destructive as **false negatives**.

False positives are wrong detection by an anti-virus where legitimate files were mistakenly identified as viruses while **False negatives** are wrong detection by an anti-virus where legitimate viruses were not detected as viruses.

Finally, antivirus software generally runs at the highly trusted kernel level of the operating system, creating a potential avenue of attack.

Over the years it has become necessary for antivirus software to **check** an increasing **variety of files**, rather than just executables, for several **reasons**:

- Powerful macros used in word processor applications, such as Microsoft Word, presented a risk. **Virus writers could use the macros to write viruses embedded within documents.** This meant that computers could now also be at risk from infection by opening documents with hidden attached macros.
- Later **email programs**, in particular Microsoft Outlook Express and Outlook, were vulnerable to viruses embedded in the email body itself. A user's computer could be infected by just opening or previewing a message.

As always-on broadband connections became the norm, and more and more viruses were released, it became essential to update virus checkers more and more frequently. Even then, a new zero-day virus could become widespread before antivirus companies released an update to protect against it.



2.3. Types of Protection Software

Depending on ***the way they fix destructive software*** these can be in the following forms: ***Anti-Virus, Anti-spyware, and Anti-spam*** Applications.

2.3.1. Anti-Viruses

- Anti-virus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software.
- Anti-virus software typically uses two different techniques to accomplish this:
 - ✓ Examining (scanning) files to look for known viruses matching definitions in a virus dictionary.
 - ✓ Identifying suspicious behavior from any computer program which might indicate infection. Such analysis may include data captures, port monitoring and other methods.
- Most commercial anti-virus software uses both of these approaches, with an emphasis on the virus dictionary approach.

2.3.2. Anti-Spyware

- These are software's that are designed to discover, detect and block spyware.
- Anti-spyware programs can combat spyware in two ways:
 - ✓ They can provide real time protection against the installation of spyware software on your computer. This type of spyware protection works the same way as that of anti-virus protection in that the anti-spyware software scans all incoming network data for spyware software and blocks any threats it comes across.
 - ✓ Anti-spyware software programs can be used solely for detection and removal of spyware software that has already been installed onto your computer. This type of spyware protection is normally much easier to use and more popular.

2.3.3. Anti-Spam

- To prevent e-mail spam, both end users and administrators of e-mail systems use various anti-spam techniques.
- None of the techniques is a complete solution to the spam problem, and each has trade-offs between incorrectly rejecting legitimate e-mail vs. not rejecting all spam, and associated costs in time and effort.
- Anti-spam techniques can be broken into two broad categories:
 - ✓ those that require actions by individuals, and
 - ✓ those that can be automated.



2.4. Methods Anti-virus Use to Identify Malware

There are several methods which antivirus software can use to identify malware.

- **Signature based detection** is the most common method. To identify viruses and other malware, antivirus software **compares the contents of a file to a dictionary of virus signatures**. Because viruses can embed themselves in existing files, the entire file is searched, not just as a whole, but also in pieces.
- **Heuristic-based detection**, like malicious activity detection, can be used to identify unknown viruses.
- **File emulation** is another heuristic approach. File emulation involves executing a program in a **virtual environment** and logging what actions the program performs. Depending on the actions logged, the antivirus software can determine if the program is malicious or not and then carry out the appropriate disinfection actions.

2.4.1. Signature-based detection

Traditionally, antivirus software heavily relied upon signatures to identify malware. This can be very effective, but cannot defend against malware unless samples have already been obtained and signatures created. Because of this, signature-based approaches are **not effective against new**, unknown viruses.

As new viruses are being created each day, the signature-based detection approach **requires frequent updates** of the virus signature dictionary. To assist the antivirus software companies, the software may allow the user to upload new viruses or variants to the company, allowing the virus to be analyzed and the **signature added to the dictionary**.

Although the signature-based approach can effectively contain virus outbreaks, virus authors have tried to stay a step ahead of such software by writing "**oligomorphic**", "**polymorphic**" and, more recently, "**metamorphic**" viruses, which **encrypt parts of themselves** or otherwise modify themselves **as a method of disguise, so as to not match virus signatures in the dictionary**.

2.4.2. Heuristics

Some more sophisticated antivirus software uses heuristic analysis to identify new malware or variants of known malware.

Many **viruses start** as a **single infection** and through either mutation or refinements by other attackers, can **grow** into dozens of slightly different strains, called **variants**. Generic detection refers to the detection and removal of multiple threats using a single virus definition.

For example, the **Vundo trojan** has several family members, depending on the antivirus vendor's classification. Symantec classifies members of the Vundo family into two distinct categories, *Trojan.Vundo* and *Trojan.Vundo.B*.



While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a **generic signature** or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie. These wildcards allow the scanner to detect viruses even if they are padded with extra, meaningless code. A detection that uses this method is said to be "heuristic detection."

2.4.3. Rootkit detection

Anti-virus software can also scan for rootkits; a **rootkit virus** is a type of malware that is designed to gain administrative-level control over a computer system without being detected. Rootkits can change how the operating system functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult to remove, in some cases requiring a complete re-installation of the operating system.

2.5. Selecting Anti-Virus Software

A good security program needs to be integrated & working actively deep in the system in order to protect it from malicious software. This means that it needs to be active from initial boot up to shutdown, scanning each process or program and how it interacts with the system.

It is therefore important when choosing a virus scanner that protects the system from all kinds of malicious software but also that it doesn't degrade the device's ability to function.

In the previous module, we have already discussed the planning and analysis that should be undertaken before any systems software is installed onto a computer. The installation of anti-virus software is no different. Each analysis step that we have covered must be undertaken to ensure that the software we choose is going to meet our needs as well as maintain compatibility with the operating system, application software and hardware. When it comes to anti-virus software however, there are other aspects to take into consideration such as:
























- The types of virus protected against
- Yearly subscription fees
- Other services available such as firewalls, SPAM management and system diagnostic software

In most cases, this information will be covered on the website of the software manufacturer.



2.6. Avast Anti-Virus Software

The screenshot below display the three Avast antivirus products with their features, from essential to complete protection

	 Free AntiVirus Essential	 Internet Security Advanced	 Premier Complete
 Anti-Malware	•	•	•
 Anti-Spyware	•	•	•
 Streaming Updates	•	•	•
 Hardened Mode	•	•	•
 CyberCapture	•	•	•
 Game Mode	•	•	•
 Behavior Shield	•	•	•
 Do Not Track, SiteCorrect, Anti-Phishing ENHANCED	•	•	•
 Wi-Fi Inspector	•	•	•
 Web / File / Mail Shield	•	•	•
 Smart Scan	•	•	•
 Passwords	•	•	•
 Software Updater	Manual	Manual	Automatic
 Ransomware Shield NEW		•	•
 Sandbox		•	•
 Real Site		•	•
 Anti-Spam		•	•
 Firewall		•	•
 Data Shredder			•
 Webcam Shield NEW			•



2.7. Installing Anti-Virus Software

The Following system requirements are recommended in order to install and run Avast! Free Antivirus on your computer:

- Microsoft Windows XP Service Pack 2 or higher (any Edition, 32-bit or 64-bit), Microsoft Windows Vista (any Edition excl. Starter Edition, 32-bit or 64-bit) or Microsoft Windows 7 (any Edition, 32-bit or 64-bit).
- Windows fully compatible PC with Intel Pentium III processor or above (depends on the requirements of used operating system version and other 3rd party software installed).
- 256 MB RAM or above (depends on the requirements of used operating system version and other 3rd party software installed).
- 210 MB free space on the hard disk, 300MB if also included Google Chrome will be installed (to download and install).
- Internet connection (to download and register the product, for automatic updates of program engine and antivirus database).
- Optimally standard screen resolution not less than 1024 x 768 pixels.

Before you begin the installation of Avast! Free Antivirus please ensures that:

- You are logged in to Windows as Administrator or as a user with administrator permissions
- All other programs in Windows are closed and not running
- Your previous antivirus software is fully uninstalled (for instructions refer to your vendor's documentation),

Once you have installed an anti-virus package, you should scan your entire computer periodically. Always leave your Anti-virus software running so it can provide constant protection.

- **Automatic Scans-** Depending what software you choose, you may be able to configure it to automatically scan specific files or directories and prompt you at set intervals to perform complete scans.
- **Manual Scans-** It is also a good idea to manually scan files you receive from an outside source before opening them. This includes:
 - ✓ Saving and scanning *email attachments* or *web downloads* rather than selecting the option to open them directly from the source
 - ✓ Scanning *flash disks*, *CDs*, or *DVDs* for viruses before opening any of the files



TIPS TO BOOST YOUR MALWARE DEFENSE AND PROTECT YOUR PC

1. Install Antivirus and Antispyware Programs from a Trusted Source

- Never download anything in response to a warning from a program you didn't install or don't recognize that claims to protect your PC or offers to remove viruses. It is highly likely to do the opposite!
- Get reputable anti-malware programs from a vendor you trust. (Microsoft Security Essentials offers free real-time protection against malicious software for your PC. Or, choose from a list of Microsoft partners who provide anti-malware software). Other reputable defenders include Avast!, McAfee, Kaspersky, Norton's, and AVG.

2. Update Software Regularly

Cybercriminals are endlessly inventive in their efforts to exploit vulnerabilities in software, and many software companies work tirelessly to combat these threats. That is why you should:

- Regularly install updates for all your software, namely your antivirus and antispyware programs, browsers (like Windows Internet Explorer), operating systems (like Windows), and word processing and other programs. Software updates repair vulnerabilities as they are discovered.
- Subscribe to automatic software updates whenever they are offered—for example, you can automatically update all Microsoft software.
- Uninstall software that you don't use. You can remove it using Windows Control Panel.

3. Use Strong Passwords and Keep Them Safe

- Strong passwords are at least 14 characters long and include a combination of letters, numbers, and symbols.
- Don't share passwords with anyone.
- Don't use the same password on all sites. If it is stolen, all the information it protects is also at risk.
- Create different strong passwords for the router and the wireless key of your wireless connection at home. Find out how from the company that provides your router.

4. Never Turn Off your Firewall

A firewall protects networked computers from hostile intrusion. It may be a hardware device or a software program. In either case, it has at least 2 network interfaces – one for the network or computer that it is protecting and one for the network that it is exposed to. Often the case is of a private network/computer and the Internet. A firewall prevents computers outside the protected area from gaining access. Windows Vista, Windows 7, Server 2008 and Linux all make use of software firewalls.



A firewall puts a protective barrier between your computer and the Internet. Turning it off for even a minute increases the risk that your PC will be infected with malware.

5. Use Flash Drive with Caution

Minimize the chance that you'll infect your computer with malware:

- Don't put an unknown flash (or thumb) drive into your PC.
- Hold down the SHIFT key when you insert the drive into your computer. Holding down "Shift" will keep the computer from auto-playing the device. If you forget to do this, click in the upper-right corner to close any flash drive-related pop-up windows.
- Don't open any files on your drive that you're not expecting.

Don't be tricked into downloading malware

Follow this advice:

- Be very cautious about opening attachments or clicking links in email or IM (Instant Messaging), or in posts on social networks (like Facebook)—even if you know the sender. Call to ask if a friend sent it; if not, delete it or close the IM window.
- Avoid clicking “Agree”, “OK”, or “I Accept” in banner ads, in unexpected pop-up windows or warnings, on websites that may not seem legitimate, or in offers to remove spyware or viruses.
- Instead, press CTRL + F4 on your keyboard. (CTRL + F4 closes the Window)
- If that doesn't close the window, press ALT + F4 on your keyboard to close the browser. If asked, close all tabs and don't save any tabs for the next time you start the browser.
- Only download software from websites you trust. Be cautious of "free" offers of music, games, videos, and the like. They are notorious for including malware in the download.



Self-Check - 2	Written Test
-----------------------	---------------------

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Write at least five kinds of protection software available for a single use device

2. _____ is used to prevent, detect, and remove malware, including but not limited to computer viruses, computer worm, trojan horses, spyware and adware.

3. _____ are wrong detection by an anti-virus where legitimate files were mistakenly identified as viruses.

4. _____ are wrong detection by an anti-virus where legitimate viruses were not detected as viruses.

5. Depending on ***the way they fix destructive software*** these can be in the following forms: _____, _____, and _____ Applications.

6. List and describe the methods antivirus software can use to identify malware.

7. When selecting anti-virus software, there are other aspects to take into consideration such as:



Answer Sheet

Score = _____

Rating: _____

Name: _____

Date: _____

Short Answer Questions

1. _____

2. _____
3. _____
4. _____
5. _____, _____, and _____
6. _____

7. _____



3.1. Firewalls

A Firewall is a software program that sits between the internet and a private network and works as a barrier to keep destructive viruses away from a computer. The purpose is to prevent unauthorised access into the company by outsiders. Data can only travel from the Internet to the network through the firewall. The software can be configured to accept links only from trusted sites.

The firewall prevents direct communication between computers outside the network (in other words, out on the Internet) and computers on the private network. It also monitors and logs everything passing between the two so as to prevent a hacker or any other unauthorised person from connecting through to your network.

3.2. Risks of Allowing Applications Through a Firewall

There are two ways to allow an application through a firewall. Both of them are risky:

- Add an application to the list of allowed applications (less risky).
- Open a port (more risky).

When you add an application to the list of allowed applications in a firewall (sometimes called unblocking) or when you open a firewall port, you allow a specific application to send information to or from your PC through the firewall, as though you've drilled a hole in the firewall. This makes your PC less secure and might create opportunities for hackers or malware to use one of those openings to access your files or use your PC to spread malware to other PCs.

Generally, it's safer to add an application to the list of allowed applications than to open a port. A port stays open until you close it, but an allowed application only opens the "hole" when needed.

To help decrease your security risk:

- Only allow an application or open a port when you really need to,
- Never allow an application that you don't recognise to communicate through the firewall.

3.3. Configuring Windows Firewall

Windows Firewall is a host firewall that is built into Windows 7. Unlike firewall devices that control traffic between networks, host firewall define which traffic types are allowed to pass between the local computer and the rest of the network.

You can configure Windows Firewall by using two separate tools.

- If you want to control inbound traffic based on its associated application, use the Windows Firewall page in Control Panel. To open this tool, open Control Panel, click System and Security, and then click Windows Firewall, as shown in Figure 3-1.

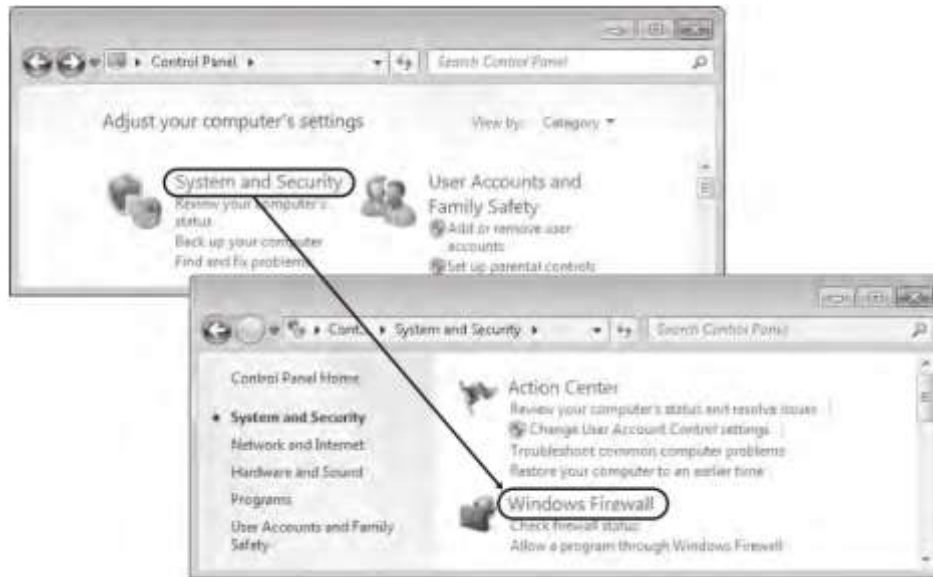


FIGURE 3-1 Accessing Windows Firewall settings in Control Panel



FIGURE 3-2 Windows Firewall page in Control Panel

- If you want to control outbound traffic, or if you want to control inbound traffic based on additional criteria such as source address or destination port, you need to use the Windows Firewall with Advanced Security (WFAS) console. To open this console, click Advanced Settings on the Windows Firewall page in Control Panel



Self-Check - 3	Written Test
-----------------------	---------------------

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. _____ is a software program that sits between the internet and a private network and works as a barrier to keep destructive viruses away from a computer.

2. There are two ways to allow an application through a firewall. Both of them are risky:

3. To help decrease your security risk:

4. If you want to control inbound traffic based on its associated application, use

5. If you want to control outbound traffic, or if you want to control inbound traffic based on additional criteria such as source address or destination port, use

Note: Satisfactory rating - 3 points

Unsatisfactory - below 3 points

You can ask your teacher for the copy of the correct answers.



Answer Sheet

Score = _____

Rating: _____

Name: _____

Date: _____

Short Answer Questions

1. _____

2. _____

3. _____

4. _____

5. _____



4.1. Updating Windows

Although Windows is designed to minimize security risks out of the box, attackers are constantly developing new security vulnerabilities. To adapt to changing security risks, improve the reliability of Windows, and add support for new hardware, you must deploy updates to your client computers.

In homes and small offices, Windows automatically downloads the newest critical updates from Microsoft, allowing computers to stay up to date without any administrative effort. This approach does not scale to enterprises, which must manage thousands of computers. In enterprises, IT departments need to test updates to ensure that they do not cause widespread compatibility problems. In addition, having each computer download the same update across the Internet would waste your bandwidth, potentially affecting your network performance when Microsoft releases large updates.

Because security threats are evolving constantly, Microsoft must release updates to Windows and other Microsoft software regularly. Deploying and managing these updates are some of the most important security tasks an IT department can perform.

4.1.1. Methods for Deploying Updates

Microsoft provides several techniques for applying updates:

- **Directly from Microsoft**

For home users and small businesses, Windows 7 is configured to retrieve updates directly from Microsoft automatically. This method is suitable only for smaller networks with fewer than 50 computers.

- **Windows Server Update Services (WSUS)**

WSUS enables administrators to approve updates before distributing them to computers on an intranet. If you want, updates can be stored and retrieved from a central location on the local network, reducing Internet usage when downloading updates. This approach requires at least one infrastructure server.

- **Configuration Manager 2007**

The preferred method for distributing software and updates in large, enterprise networks, Configuration Manager 2007 provides highly customizable, centralized control over update deployment, with the ability to audit and inventory client systems. Configuration Manager 2007 typically requires several infrastructure servers.



4.1.2. Windows Update Client

Whether you download updates from Microsoft or use WSUS, the Windows Update client is responsible for downloading and installing updates on computers running Windows 7 and Windows Vista. The Windows Update client replaces the Automatic Updates client available in earlier versions of Windows. Both Windows Update in Windows 7 and Automatic Updates in earlier versions of Windows operate the same way: they download and install updates from Microsoft or an internal WSUS server. Both clients install updates at a scheduled time and automatically restart the computer if necessary. If the computer is turned off at that time, the updates can be installed as soon as the computer is turned on. Alternatively, Windows Update can wake a computer from sleep and install the updates at the specified time if the computer hardware supports it.

The Windows Update client provides for a great deal of control over its behavior. You can configure individual computers by using the Control Panel\System and Security\Windows Update\Change Settings page.

After the Windows Update client downloads updates, the client checks the digital signature and the Secure Hash Algorithm (SHA1) hash on the updates to verify that they have not been modified after they were signed by Microsoft. This helps mitigate the risk of an attacker either creating malware that impersonates an update or modifying an update to add malicious code.

4.1.3. How to Check Update Compatibility

Microsoft performs some level of compatibility testing for all updates. *Critical updates* (small updates that fix a single problem) receive the least amount of testing because they occur in large numbers and they must be deployed quickly. Service packs (large updates that fix many problems previously fixed by different critical updates) receive much more testing because they are released infrequently.

Whether you are planning to deploy critical updates or a service pack, you can reduce the chance of application incompatibility by testing the updates in a lab environment. Most enterprises have a Quality Assurance (QA) department that maintains test computers in a lab environment with standard configurations and applications. Before approving an update for deployment in the organization, QA installs the update on the test computers and verifies that critical applications function with the update installed.

Whether you have the resources to test updates before deploying them, you should install updates on pilot groups of computers before installing the updates throughout your organization. A pilot group is a small subset of the computers in your organization that receive an update before wider deployment. Ideally, pilot groups are located in an office with strong IT support and have technology-savvy users. If an update causes an application



compatibility problem, the pilot group is likely to discover the incompatibility before it affects more users.

4.1.4. How to Install Updates

Ideally, you would deploy new computers with all current updates already installed. After deployment, you can install updates manually, but you'll be much more efficient if you choose an automatic deployment technique. For situations that require complete control over update installation but still must be automated, you can script update installations.

4.1.5. How to Verify Updates

Microsoft typically releases updates once per month. If a computer does not receive updates, or the updates fail to install correctly, the computer might be vulnerable to security exploits that it would be protected from if the updates were installed. Therefore, it's critical to the security of your client computers that you verify updates are regularly installed.

4.1.6. How to Remove Updates

Occasionally, an update might cause compatibility problems. If you experience problems with an application or Windows feature after installing updates and one of the updates was directly related to the problem you are experiencing, you can uninstall the update manually to determine whether it is related to the problem.

If removing the update does not resolve the problem, you should reapply the update. If removing the update does solve the problem, inform the application developer (in the case of a program incompatibility) or your Microsoft support representative of the incompatibility. The update probably fixes a different problem, so you should make every effort to fix the compatibility problem and install the update.

4.2. Updating Anti-Virus Software



Self-Check - 4	Written Test
-----------------------	---------------------

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. Although Windows is designed to minimize security risks out of the box, attackers are constantly developing _____.
2. To adapt to _____, _____, and _____, you must deploy updates to your client computers.
3. Because _____ are evolving constantly, Microsoft must release updates to Windows and other Microsoft software regularly.
4. list and explain techniques for applying updates provided by Microsoft:
 - _____

 - _____

 - _____

5. _____ (small updates that fix a single problem) receive the least amount of testing because they occur in large numbers and they must be deployed quickly.
6. _____ (large updates that fix many problems previously fixed by different critical updates) receive much more testing because they are released infrequently.

Note: Satisfactory rating - 3 points **Unsatisfactory - below 3 points**
You can ask your teacher for the copy of the correct answers.



Answer Sheet

Score = _____

Rating: _____

Name: _____

Date: _____

Short Answer Questions

1. _____

2. _____, _____, and _____,

3. _____

4.

- _____

- _____

- _____

5. _____

6. _____



5.1. Internet Security

We have already discussed some of the functionality of anti-virus and firewall software when it comes to protecting your computer network. Since many of these threats come from the Internet, many web browsing software programs contain inbuilt security settings which allow you to restrict or block access to sites before they can become a problem.

In Microsoft Internet Explorer, security is handled by division of sites into restricted zones. This means that different web sites can have different security levels.

There are four Internet Security Zones, and within each zone a different security level can be set.

5.1.1. Security Zones

You can tell which zone the current Web page is in by looking at the right side of the Internet Explorer status bar. Whenever you open or download content from the Web, Internet Explorer checks the security settings for that Web site's zone.

- Search for and view any website.
- Look at the bottom right of the screen:

We will access a screen in Internet Explorer which explains these zones, and where you can make changes to the zone settings.

5.1.2. Viewing Security Zones

If you are on a PC where changes can be made, you change the Internet Zones through **Tools, Internet Options, Security**

- Choose Tools, Internet Options.
- Click on the Security tab.

The top of the dialog box displays the four available security zones. The remainder of the dialog box allows you to choose a security level for that zone.



Figure 5-1 The Internet zone with medium security level



5.2. Different Security Zones

There are four different zones:

- **Internet zone:** By default, this zone contains anything that is not on your computer or an intranet, or assigned to any other zone. The default security level for the Internet zone is Medium.
- **Local intranet zone:** This zone typically contains addresses that you have access to such as shared network drives, and local intranet sites.
- **Trusted sites zone:** This zone contains sites that are considered trustworthy - sites where you can usually download or run files from without worrying about damage to your computer.
- **Restricted sites zone:** This zone contains sites that are not trusted - that is, sites that you're not sure whether you can download or run files from without damage to your computer or data.

Settings can be customized within a zone from Low, Medium Low, Medium, and High. If you are in a workplace or college, these security decisions have probably been made for you and it is unlikely that you can change these. However for the purposes of this exercise, we will view the different zones and their security settings.



Self-Check - 5	Written Test
-----------------------	---------------------

Directions: Answer all the questions listed below. Use the Answer sheet provided in the next page:

1. In _____, security is handled by division of sites into restricted zones. This means that different web sites can have different security levels.
2. List and describe the four Internet Security Zones

- _____:

- _____:

- _____:

- _____:

3. Internet Security Zones Settings can be customized within a zone from _____, _____, _____, and _____.



Answer Sheet

Score = _____

Rating: _____

Name: _____

Date: _____

Short Answer Questions

1. _____,

2.

- _____:

- _____:

- _____:

- _____:

3. _____, _____, _____, and _____.

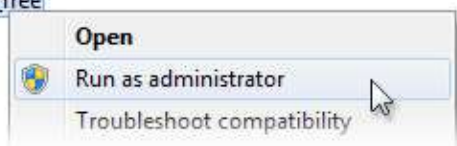


Operation Sheet - 1

Installing Avast! Free Antivirus

To prevent Avast! Free Antivirus from being incorrectly installed or aborted unexpectedly. When you are ready, proceed as follows:

1. Firstly download the Avast! Free Antivirus from the Avast! Website and save it to your computer, in a location where you will easily be able to locate it. For example save the downloaded setup file `avast_free_antivirus_setup.exe` on your Windows Desktop.
2. Locate the downloaded setup file `avast_free_antivirus_setup.exe` (depending on your system preferences, the file extension may be hidden), on your Windows Desktop for example. Now, in case you are logged in to:



- Windows 7 or Windows Vista as a user with administrator permissions, right-click on the setup file and choose 'Run as administrator' from the context menu,
- Windows XP as Administrator or as a user with administrator

permissions, or you are logged in to Windows 7 or Windows Vista as Administrator (i.e. not a user with administrator permissions), double-click the setup file to begin the installation process,

If prompted by User Account Control dialog for permissions, click 'Yes' (or 'Continue' in Windows Vista) to begin the installation process.



For a few seconds you will briefly see the setup process copy the installation files to your computer.

When Avast! Setup Wizard starts you will see a welcome screen. Preferred language for the installation can be changed by clicking on the current language shown on the top right corner. Before continuing with the installation of Avast! Free Antivirus please read the User License Agreement.



At the bottom of the welcome screen you can choose whether you wish to install Google Chrome. By ticking the checkbox 'Make Google Chrome my default browser', you can also select, if it should be opened as your default

browser. By ticking the checkbox 'Make Google Chrome my default browser', you can also select, if it should be opened as your default



web browser when accessing the Internet. For details, please read enclosed Terms of Use and Privacy Policy.

Then choose what type of installation you prefer:

- **Regular Install** or **Custom Install**

Regular Installation of Avast! Free Antivirus


1. Click the 'Regular Installation' button in the middle of the welcome screen to proceed with default installation of Avast! Free Antivirus in preferred language and with minimal user interaction during the setup process.
2. You will now be prompted to Accept the End User License Agreement by Clicking on the 'Continue' button.
3. The Avast! Setup Wizard will create a system restore point, then will display an installation progress bar,



4. When installation has successfully completed click 'Done'. Now Avast Free Antivirus will perform a quick scan of your system. Depending upon the speed of your machine, it may take a few minutes to complete.

Avast! Free Antivirus is now installed on your computer and ready to use. But it works for 30 days in trial mode after installation. During this period you need to register to get your free license key to continue to use it and stay protected.



Avast! User interface is accessible via orange ball icon  in your system tray or orange shortcut icon on your Windows Desktop.



Operation Sheet - 2

Running and Scheduling Avast! Free Antivirus





LAP Test	Practical Demonstration
-----------------	--------------------------------

Name: _____ Date: _____

Time started: _____ Time finished: _____

Instructions: Given necessary templates, tools and materials you are required to perform the following tasks within --- hour.



List of Reference Materials