A study of managing antivirus tools used for personal computers in Pune city

A Thesis submitted to
Tilak Maharashtra Vidyapeeth
Pune

For the Degree of

Doctor of Philosophy (Ph. D.)

Under The Faculty of Management

By

Mrs. Sheetal Sandeep Patil

Under the Guidance of

Dr. Prasanna G. Deshmukh

February 2018

DECLARATION

I hereby declare that the thesis entitled “A study of managing antivirus tools used for personal computers in pune city” completed and written by me has not previously formed the basis for the award of any Degree or other similar title upon me of this or any other Vidyapeeth or examining body.

Date :

Place:

Mrs. Sheetal Sandeep Patil

Research student

C E R T I F I C A T E

This is to certify that the thesis entitled "**A study of managing antivirus tools used for personal computers in pune city**" which is being submitted herewith for the award of the Degree of Vidyavachaspati (Ph.D.) in Management of Tilak Maharashtra Vidyapeeth, Pune is the result of original research work completed by Smt. Sheetal Sandeep Patil under my supervision and guidance. To the best of my knowledge and belief, the work incorporated in this thesis has not formed the basis for the award of any Degree or similar title of this or any other University or examining body upon her.

Dr. Prasanna G. Deshmukh

(Research Guide)

Place :

Date :

ACKNOWLEDGEMENT

"Gratitude makes you to realize the paradise of life". I would like to express my sincere gratitude to all of them who supported me in completion of doctoral dissertation.

I am extremely grateful to my research guide, **Dr. Prasanna Deshmukh**, Principal and Head, Anantrao Thopate College and Research Center, Bhor - Pune for his valuable guidance, scholarly inputs and consistent encouragement I received throughout the research work. A person with great vision and positive disposition, Sir has always made himself available to clarify my doubts despite his busy schedules and I consider it as a great opportunity to do my doctoral programme under his guidance and to learn from his research expertise. Thank you Sir, for all your help and support.

I thank Prof. Yashodhan. Soman, Director, Keystone School Of Engineering for motivating and cooperating me for research work . I sincerely thank Prof. Manikrao Dhore, Professor, Vishwakarma Institute Of Technology for his valuable suggestions, guidance and concise comments on my research work time to time and Prof. Rajesh Barapte for his consistent support. I am also thankful to faculty members of the Keystone School of Engineering, Dr. Manisha Kumbhar who have been very kind enough to extend their help at various phases of this research work..

I sincerely thankful to Hon. H. K. Abhyankar for his valuable guidance and motivation for completion of thesis work.

Finally, I thank my Aai (Mrs. Kamal Shinde), Pappa (Mr. Shripati Shinde) whose enthusiasm and inspiration transformed my dream of doctorate degree into reality. Also Appasaheb (Mr. Pandurang Patil) and Aai (Mrs.Shalini Patil) for their unconditional support. I am very much indebted to my family, my husband and my better half Mr. Sandeep Patil, my daughters Tejal and Chaitrali who supported me in every possible way to see the completion of this work.

Above all, I oblige it all to Almighty God for granting me the wisdom, health and strength to undertake this research task and enabling me to its completion.

Mrs. Sheetal Sandeep Patil

List of Tables

List of Charts

List of Figures

List of Abbreviations

VIRUS	: Vital Information Resources under Siege
PC	: Personal Computer
DoS	: Denial of service Attack
DNS	: Domain Name System
AV	: Antivirus Tool
TS	: Total Security
IS	: Internet Security
VPN	: Virtual Private Network
OS	: Operating System
TCP	: Transmission Control Protocol
ICT	: Information and Communication Technologies
VB	: Virus Bulletin

Chapter 1

INTRODUCTION

"We trust that everyone in this world has the right to be free of cybersecurity fears." ***Eugene Kaspersky*** *Chairman and CEO of Kaspersky Lab.*

1.1 Introduction

In the current world computers are very essential part of our life. It's almost impossible to imagine our life without computer. The uses of computer are increased day by day. As a result of this computer is important constituent of everybody's modern home having equal importance as television and telephone.

1.2.Usage of personal computer

A personal computer is a small, relatively inexpensive computer designed for use by one person at a time. It can be a in the form of desktop computer, laptop, notebook, palmtop or tablet. With the decrease in size it has become very convenient to carry and use them anywhere we are. In most of the cases the whole family shares the same PC. Every family member needs the PC to accomplish different task depending upon their needs.

Today, everything required in our everyday life can be fulfilled with few simple clicks using internet. For example we can

- Order breakfast, lunch or dinner online
- Read newspapers online
- Book movie tickets
- Watch movies and videos on You tube
- Listen to music through sound cloud
- Read novels and books through e-books
- Play games
- Can keep in touch with people through social media sites like Facebook, twitter, Instagram
- Mail documents
- Shop online

- Watch the recipes online
- Do Net banking
- Apply for jobs
- Apply for admission
- Apply carpooling using Uber and Ola applications
- Try for car pooling
- Book bus/railway tickets online
- Pay tax, insurance, phone bills, mobile recharge, electricity bills
- Plan for picnic and track the path using Google Map

As a result technology interference in human life has increased the dependence on functionality and reliability of personal computers. Also personal computer users represents large portion of computer users today. Typically all the family members share the one common PC and they are from different ages, positions and computing backgrounds having ideal environment for computer viruses to rise. By comparing the increasing number of personal computer users with increasing number of computer viruses each year we can easily realize the growing threat of computer virus towards personal computer users.

Computer users don't usually think about problems that might erupt due to virus infection till they actually face it. People presume that maintenance is just for vehicles but they ignore the fact that every personal computer needs protection and maintenance. An infected PC accounts for loss in productivity hours and is a serious concern.

1.3. Computer virus the growing threat

To put in simple terms, the computer virus is program that owns the capability to copy itself and infect a computer automatically without any user interaction. It spreads across the disks and networks by making copies of itself, usually surreptitiously. Virus generally behaves like parasites means they alter another item so that when this file is executed or run the virus becomes active.

There are various types of threats to PCs from different sorts of programs like spywares, worm, Trojans, etc., commonly known as Malware. 'PC Virus' is a term frequently utilized as a catch-all term by many for PC worms, Trojans, spyware, sneakers, sniffers, bots, adware, malware, and so on.

When a computer virus settles in a system, it can:

- Corrupt the system files.
- Monitor or spy on the information that is being sent, received or accessed from your computer.
- Steal sensitive information like passwords, PIN numbers, etc.
- Viruses can also affect the normal functioning of your computer by slowing it down or wiping out data.
- Open access for hackers to perform remote activities.

Even when you are using a computer for checking e-mails, browsing websites or sharing data using USB drives there is a chance of getting virus infection. Virus can enter your computer through CDs, USB drives, infected websites, e-mail attachments, pirated software, shareware or through networks.

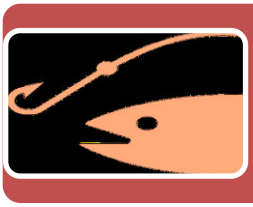
"The first PC virus that spread to large number of PCs and was in-the-wild was C-Brain developed by two brothers from Pakistan in 1986. Today, with the widespread use of Internet and extensive use of computers even by non-technical professionals the situation is far more favorable for cyber criminals to utilize and thrive upon this opportunity." (Computer viruses and what they mean to you)

These days, you can't generally tell if a site is perfect or riddled with malicious codes. Only visiting to a website page can automatically drop a malicious code in your PC. Also, this may not just occur for lesser known sites but even trusted and genuine sites are compromised by hackers to target unaware users. "November the third, 1988, was named as 'Black Thursday' after the Internet experienced a systematic attack from the 'Internet worm'. Roughly 70% of the interconnected systems were out of order. Twelve years later the well known site Yahoo.com suffered from denial of service (DoS) attack and a huge number of users couldn't access their emails. This was followed by an eminent financial organization accidently permitting all its online customers access to all customers records – this clear breach of confidentiality appeared after an upgrade of web banking software." (Computer viruses and what they mean to you)

“Eleven years later, the state of art Internet Technology is facing mammoth security challenges. The threat landscape continues to evolve as well as grow exponentially. As PCs and other digital devices inch nearer to getting to be distinctly key parts of our lives, one is overwhelmed with a considerable measure of questions regarding viruses, Internet related threats, and PC security.” (Computer viruses and what they mean to you)

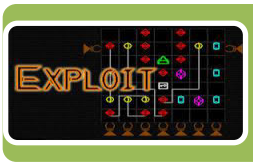
“When researchers were still dabbling with computers they experimented with programs that could replicate and copy themselves from one computer to another automatically. Developed in the early ‘80’s, these programs were quite same as PC viruses with the main difference being that they were made for the sole reason of analysis and exploration.” (Computer viruses and what they mean to you)

The current internet user base in India is whopping 400 million and is expected to reach 500 million by 2016. The list of advantages that Internet has for us is an exhaustive one and so is the list of perils it devises. This has turned Internet into a thriving lair for viruses. Following figure 1.1 are the most common types of threats on internet that most people fall prey.



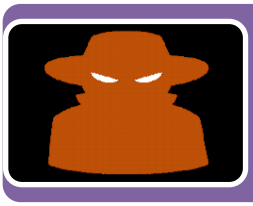
Phishing Attacks

is defined as the fraudulent act of accquiring private and sesitive information such as user names, passwords, credit/debit card information etc



Exploit

is a piece of malware that takes an advantage of bug, glitch or vulnaribility in software



Spyware

are malicious software that secretly monitor user's activities and steal sensitive information from infected computer

Keyloggers

A form of spyware which captures and records user keystrokes and trasmits it to remote computer

Trojan Horse

is seemingly benign program that when activated causes harm to computer system

Drive by Download

refers a malicious download to a computer or device that occurs without the owner's consent/knowledge

Malware Attack

can infect your computer with the help of malicious links posted by hackers

Malvertising

is malicious advertising is use of online advertising to spread malware

Spam

is made of those pesky, unsolicited emails that clog our inbox

Zero Day Virus

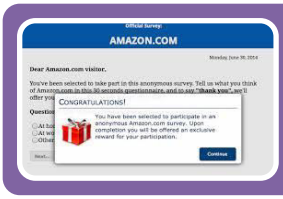
Cyber criminals take advantage of flaw in a piece of software and expoilt that vulnerability launcing an attack which antivirus tool can not detect

Identity Theft

Is unauthorized collection of personal information and it's subsiquent use for criminal reasons

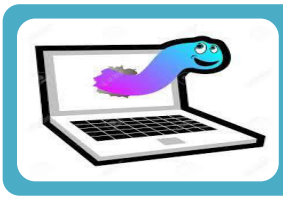
Clickjack Attack

is defined as a malicious technique used by an attacker to record the infected user's click on the internet



Fake surveys

Scammers use great offers to lure users into their trap with intetion to infect your computer to collect personal credentials



Worm

is a standalone and selfreplicating program on the internet

Ransomeware

Makes the system nonfunctional by encrypting the computers data until the victim agrees to pay ransom

Rouge Antivirus

is a scareware that disguises itself as a genuine software but performs malicious activities on user's machine

Rootkit

is a program that in itself is not harmful but helps viruses and malware to hide from antivirus software

Figure 1.1 common types of threats on internet that most people fall prey

1.4 Demonetization leads to spurt in net banking and digitalization

On eighth November 2016, Prime Minister Narendra Modi, in a sudden address to the nation, declared that Rs 500 and Rs 1,000 denomination notes are being withdrawn from midnight. He said that such notes will get to be "mere paper"(India Today, 2016).

This is a step to contain the menace of black money and to empower the poor people in India for their rights. With the promotion of a cashless economy by the Government, more and more people are likely to embrace digital modes of transactions. Many users are trying out these modes for the first time. Net banking has revolutionized the way we manage our bank accounts. Internet banking has made our lives easier by letting us bank from the comfort of our phones, desktops and laptops. It offers the services such as

- Account statements
- Alerts on account
- Ordering of cheque books
- Monitoring of term deposits
- Balance checking
- Fund transfer & bill payments
- Access to loan statement
- Access to transaction history
- eCommerce transactions
- Book a locker & a lot more....

But how exactly can we ensure the safety of our transactions is issue of concern.

Net banking reaps fruits of India's digital embrace. Net banking in India is growing like never before.

1.5 Perils of internet usage on children

1.5.1 India Ranks Third on Global Cyber Bullying List

Children in India revealed the third most online bullying rate, after China and Singapore, among the 25 nations reviewed under recently commissioned project by Microsoft Corporation to comprehend the worldwide pervasiveness of online bullying. In India, the overview demonstrated that 22% of children reported mean or unfriendly treatment, 29% were made fun of or teased and 25% were called mean names. The review additionally found that 70% of children said that they know a considerable measure or something

about internet bullying, while 79% were very or somewhat stressed about the phenomenon. 77% announced being bullied online and/or offline. "India is one of the few nations where the rates of online and offline bullying were equal," the overview said (India ranks 3rd in cyber Bullying)

'India is the third greatest Facebook market with almost four crore, 98 lakh Facebook users as per the social media organization Socialbakers. India may have reason to celebrate its rising online internet use rankings, however it is yet to deal with its potential negatives, particularly for teenagers, who form of the internet users in the country. Semiocast, an online social media tool, has rated India as the 6th highest user of Twitter. While all inclusive the negative side of unmitigated utilization of online usage is articulated, India has embraced social media without being too bothered about its possible hazards.' (side, 2012)

A Microsoft study early last month alerts when it revealed that over half of the kids in India utilizing the internet were either threatened or harassed online. The 'Global Youth Online Behavior Survey' led by Microsoft, uncovered that 53% of the studied children aged between 8 and 17 in India admitted they were victims of cyber bullying.' (side, 2012)

Jacqueline Beauchere, author of the 'Global Youth Online Behavior Survey' stated, "With the growing popularity of social networking, it is not shocking that we are seeing another breed of socially engineered dangers. When it comes to bullying, technology now provides a new platform on which behaviors ranging from meanness to cruelty can occur."

Anup Girdhar, a cyber crime investigator, said that there were a few instances of impersonation that happened through social networking sites. "This might be triggered by jealousy or to harm someone's reputation," he asserted. He exhorts not posting photos on social networking sites since fraudsters often morph photos and put them on different sites (India ranks 3rd in cyber Bullying).

India earlier witnessed stray social media negativity in one case leading to a tragic suicide. Last September, an MA student of Indian Institute Management (IIM), Bangalore committed suicide after her boyfriend dumped her on Facebook.

A recent (Tim Rains, Director of Trustworthy Computing at Microsoft., 2013) 'Tata Consultancy GenY Survey 2011-2012' of almost 12,300 secondary school students across 12 Indian cities found that 85% of the students use Facebook. Dr Sameer Malhotra, head, department of mental health at Max Healthcare, said that numerous students whom he counseled at schools experienced cyber bullying through social media sites. (side, 2012)

He said that these sites have tremendous effect on the self-esteem and mindset of child. On an average, Dr Malhotra treats a few cases identifying with emotional stress caused by social network sites every day. He called attention to that many children were addicted to Facebook and spent almost six to seven hours online. (side, 2012) This is the serious threat and should be tended to.

1.5.2 Cyber bullying is characterized as "the utilization of electronic media to bully a person, typically by sending messages of an intimidating nature." It is described in figure1.2

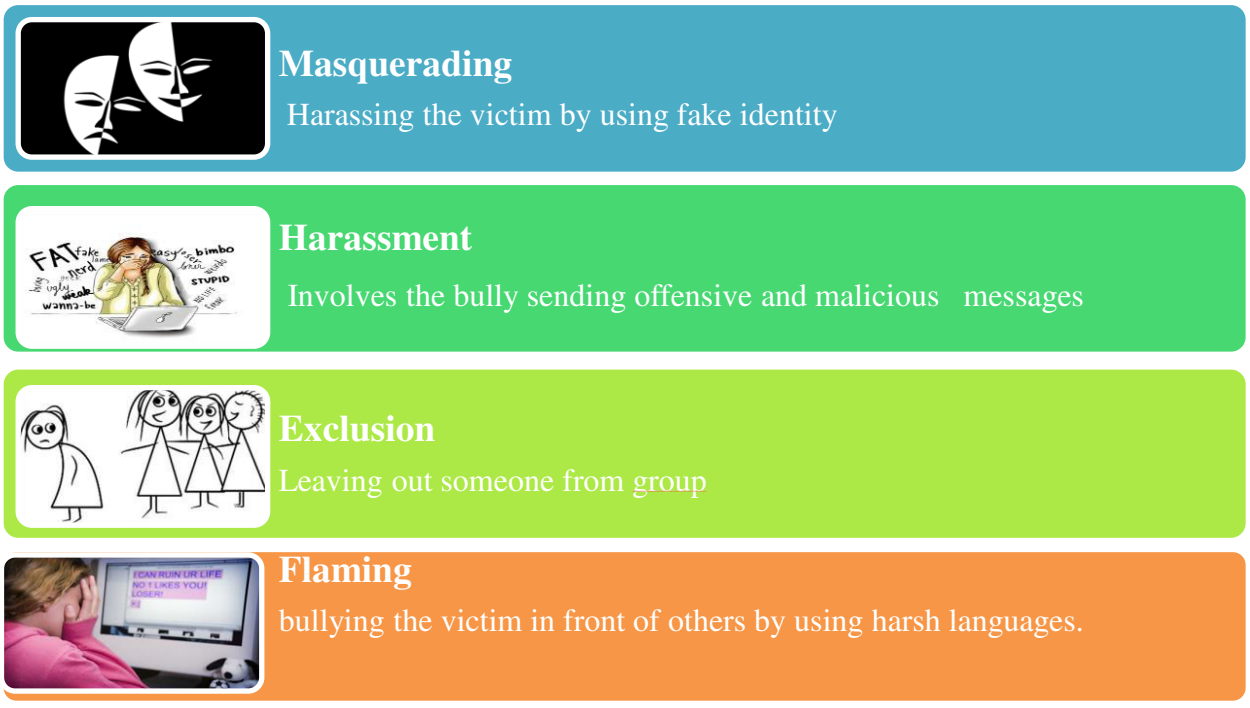


Figure 1.2 Different forms of cyber bullying

1.5.2 Effects of Cyber bullying

Cyber bullying can have many negative ramifications on the victim. It influences the academic career of child but also adversely affects their physical, social, and mental well

being. Mainly every child is a limited edition of a God and should be protected preciously.

Our child is our asset and nothing in this world is more vital than our child. Unlike adults, children's naivety and inexperience pose a greater peril. It is very common to hear incidents in which a child fell prey to a stranger pretending to be another child. To avoid this many parent stop their child to use internet but which is not an ultimate solution because many school adopt online assignments as teachings aids making complete internet-blackout impossible. As a parent, we probably have concerns about our child's online safety. With the influx of social networking sites and easily available computers, there is pressing concern on whether their action and behavior online is appropriate or not. It's our ethical duty to protect our child from the online threats without taking ceaselessly their flexibility of surfing on the web. Each parent is concerned about the kid's online wellbeing which is a new challenge in upbringing children in this information technology era.

So to put it plainly, some sort of security shield is required which guarantees guardians that their children utilize the Internet valuably without getting presented to any of its threats like cyber bullying or getting connected with dangerous individuals.

1.6 Need of Antivirus Tool

1.6.1 Way to manage a risk of valuables in our personal life

In personal life we invest in various insurance plans related to life, health, home, travel, accident and our vehicles to manage the risk and to invest money. When we purchase protection, we exchange the cost of a potential misfortune to the insurance agency in return for an expense, known as the premium. Insurance companies invest the funds securely, so it can grow, and pay out when there's a claim from policy holder. These insurance policies allow you to provide the right security and protection for your family, your health, asset from unavoidable circumstances.

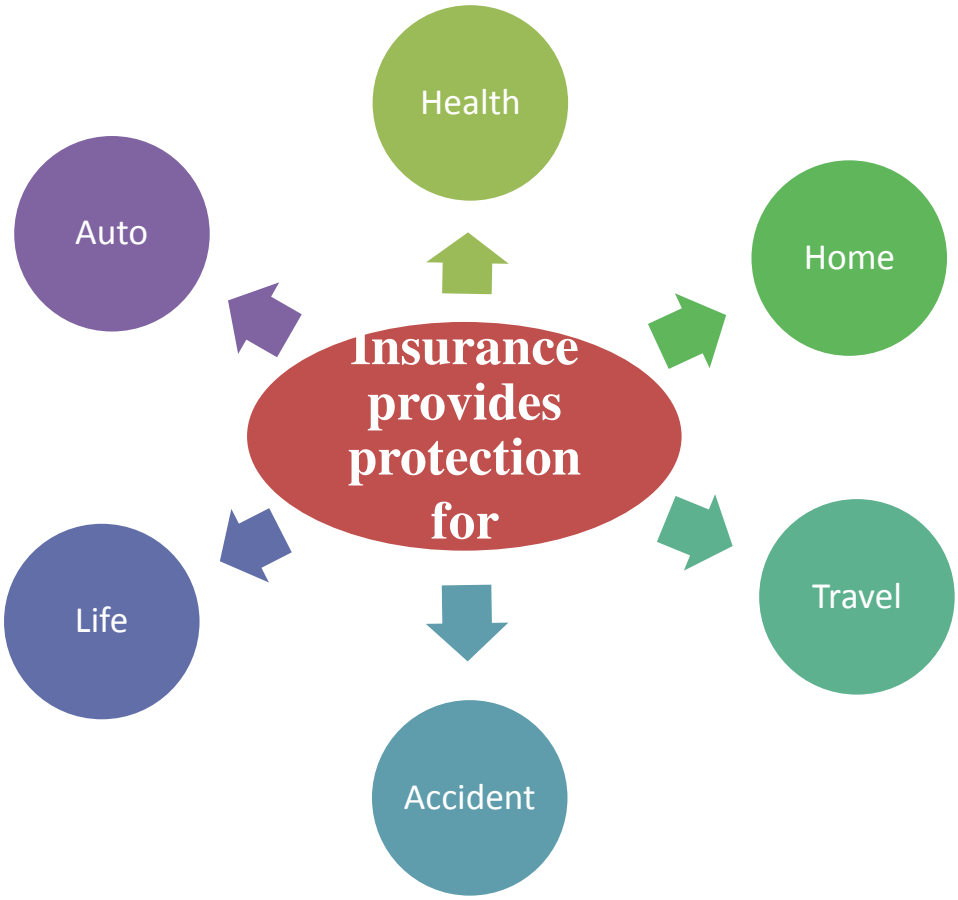


Figure 1.3 Role of insurance in personal life

1.6.2 Way to manage a risk of threats in digital life

In a similar manner, in your digital life, we depend on computers, tablets & laptop, when we're surfing, socializing, banking & shopping online.

That's why antivirus tool is needed to provide security solutions to protect what matters most is data, privacy, children, money and more. If each personal computer user invest few money on trusted antivirus, the hours saved will be worth free.

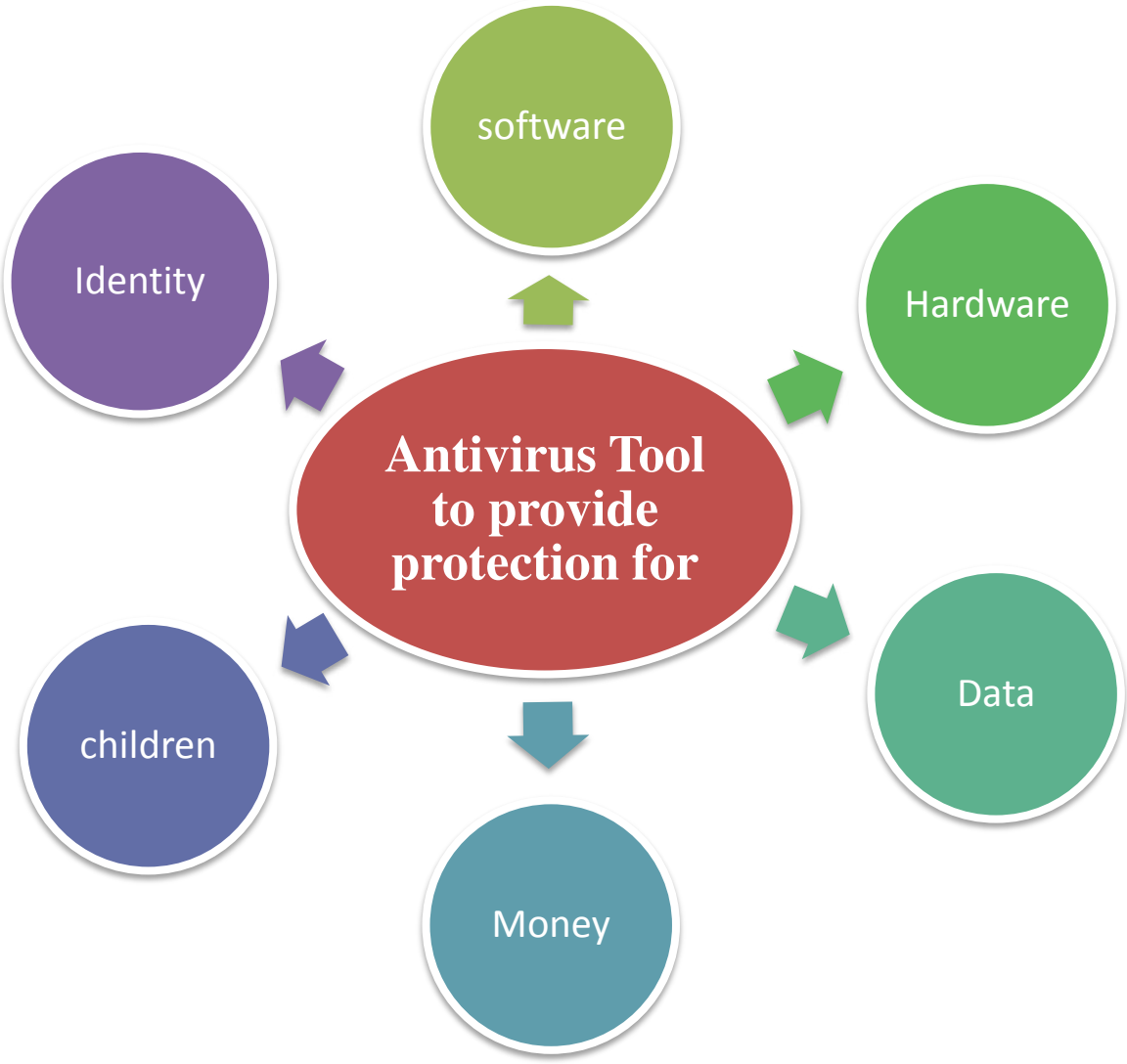


Figure 1.4 Role of antivirus tool in digital life

1.7 Common myths that stop personal computer users from using an antivirus tool

Latest security intelligence report has revealed the fact that 24 % of worldwide PCS and 30% of Indian PCS are unprotected. Microsoft released new research as a part of its Security Intelligence Report, volume 14, which takes a closer look at the significance of running up to date antivirus tool on personal computer (Tim Rains, Director of Trustworthy Computing at Microsoft., 2013). The research showed that, on average, PCs without antivirus tool are 5.5 times more likely to be infected.

Figure 1.5 Security intelligence report of worldwide computers

(Tim Rains, Director of Trustworthy Computing at Microsoft., 2013)

In India large numbers of computer users are not using antivirus tools due to following myths.

1. I only visit 'safe' websites.

   There is common misconception or phenomenon in country is that "I visit only safe websites and I don't go to bad websites" but the truth is that there is no safe website anymore on the internet or there is no safe heaven on the internet because Viruses and hackers have always find new ways to infiltrate legitimate and trusted website in the recent pasts. Experts anticipate that the frequency and velocity of cyber attacks will rise very high in years to come. There will be numerous drive by downloads, password breaches, secured service layered breaches (SSL breaches). Completely secured websites are now things of past. You need to be

protected from known viruses but also you need to shield from unknown threats. A zero day virus or new malwares could attack your personal computer before your antivirus software if any installed can find solution of it. And if it is not installed then you may be attacked by anyone, anytime, anywhere from the world.

2. Security software slows down your system.

   This is common complaint that antivirus software installed on personal computer may reduce performance of personal computer which results in slow down your system. However there are many tests in the past that has proved that installation of antivirus software will not affect the speed of system. Also the modern encryption methods are designed to utilize bare minimum resources. The main reason behind this is multiple scans or multiple applications that are running on your PC simultaneously may be the cause of slow PC. If a current running program does not meet minimum system requirement then it may slow down your PC. Always keep an eye for every installed program on your computer for system requirement such as ram, hard disk space and graphical resolution.

3. You don't have any data that is useful to hackers and this can't happen to me, only rich people are targeted

   Lot of people thinks that their data is not useful for hackers. Hackers do not care about you personally or they may not be interested in your personal address. So even if you think that you're not important or that your personal or financial data is insignificant, a potential identity theft or IT criminal can still exploit the little information discovered about you. If the same data is in bulk for example data of thousands of users then it may be important for them. They may misuse your personal data for some financial gain or can sell it to malicious parties. Everyone who goes online always have a few information which is insecure. Commonly the users who grasp this sort of deduction would prefer really not to lose time for management of risk related with digital asset.

   So stop thinking that nobody will attack your computer and the data stored on it. As long as you have a digital identity, you are a valuable target. And if there is no important data for a potential criminal on your system, they still can use your device in their own malicious purposes.

4. Why to invest money in antivirus tool if we get it free of cost downloaded from net

   There are many companies on the internet which provides free antivirus software which we can easily download from internet. The main advantage is its price. But nothing is free in this world. For example in practical life also if somebody wants to market or sale any product, they always provide free sample for the customer. It serves two purpose marketing and testing. In similar manner antivirus companies provide their antivirus tools free of cost so as to test and advertise their products which are provided for limited period after that you are forced to upgrade to the full paid version. Hackers may piggyback malwares through this free antivirus. Again these products are providing you the illusion of security which will not cover your system, your online actions, and your financial and personal data. In future if you get infected then this free antivirus may prove very expensive to you. And also free antivirus solution will not be able to prevent ransomware or other widespread malware attacks and security breaches.

5. I set strong and complex password to my account, so I will be OK

   Yes it is very essential step that you set a strong password for all your online accounts which may be face book, email, bank account or any account related to online stuff. Also your password should be unique and separate for each account and you have to keep on changing your accounts frequently otherwise cyber crook will have access to your entire digital asset just by breaching one of these accounts. However these unique and complex passwords are difficult to remember. And suppose if we are having tens of digital accounts then setting these passwords, changing them constantly and still remembering them can increase burden. To summarize, just to set a complex password is one of the many security layers that will keep safe but not completely bulletproof. Also the password will control the access but not prevent the malwares.

6. I only open emails from my friends, I only download and access information from trusted sources. My social networks are safe places. This keeps me protected.

   Most of the common misconception is that I open emails of my friends only and I download attachment from trusted source so I am safe. But the reality is exactly

different. Even if we access and download from trusted source we are still vulnerable to online dangers. Online criminals can place malicious contents like drive by downloads and pop up ads on safe websites and social media accounts. Another risk is that the social media is almost full with fake profiles created by cyber criminals and which are used to collect personal information about others.

To summarize, the main problem with these cyber security myths is that they make you drop your guard and to fall in false sense of security. Today most of the internet users are having safety awareness so malicious hackers piggyback on them by placing themselves in your shoes and by disguising themselves and their plans as legitimate entities. So to remain safe on the internet antivirus tool is utmost important.

1.8 Selection of antivirus tool

The commanding growth in the selection of available antivirus tool is no accident. As computers advance and implement new exciting and advanced features, hackers also invent new techniques that can reach you in multiple ways making today's computers more vulnerable. Hence selection of best antivirus tool is very important decision that should be taken in careful consideration. Virus can attack in many forms, infiltrating your PC without any indication. While selecting an antivirus, it is very important to ensure that your all devices are protected including mobile phones, as one compromised device can be gateway into your entire home network resulting to the infection of computers and cellular phones and more.

Because viruses can attack any time and from anywhere without warning, it's very important to ensure that antivirus tool guard your devices continuously without initiating a scan. Continuous protection assures that as a virus attempts to penetrate, it is caught and eliminated.

Most of the antivirus tools offer much more than active and manual scanning of computer system, adding extra additional features that can transform personal computer into impenetrable fortress. Which include email protection that warns you about phishing attempts and suspicious files as well as privacy oriented features such as VPNs (Virtual Private Networks) which encrypt your network data and protect your privacy. Many top antivirus companies are providing browser sandboxing which creates virtual environment

and executes your browser within this environment inside your PC. Hence any file you download or gets downloaded from browser remains isolated in sandbox environment. So even if any infection does take place from down load, it will remain confined inside this virtual environment without affecting real PC. And once you close the browser any changes that might have occurred in the environment will be deleted.

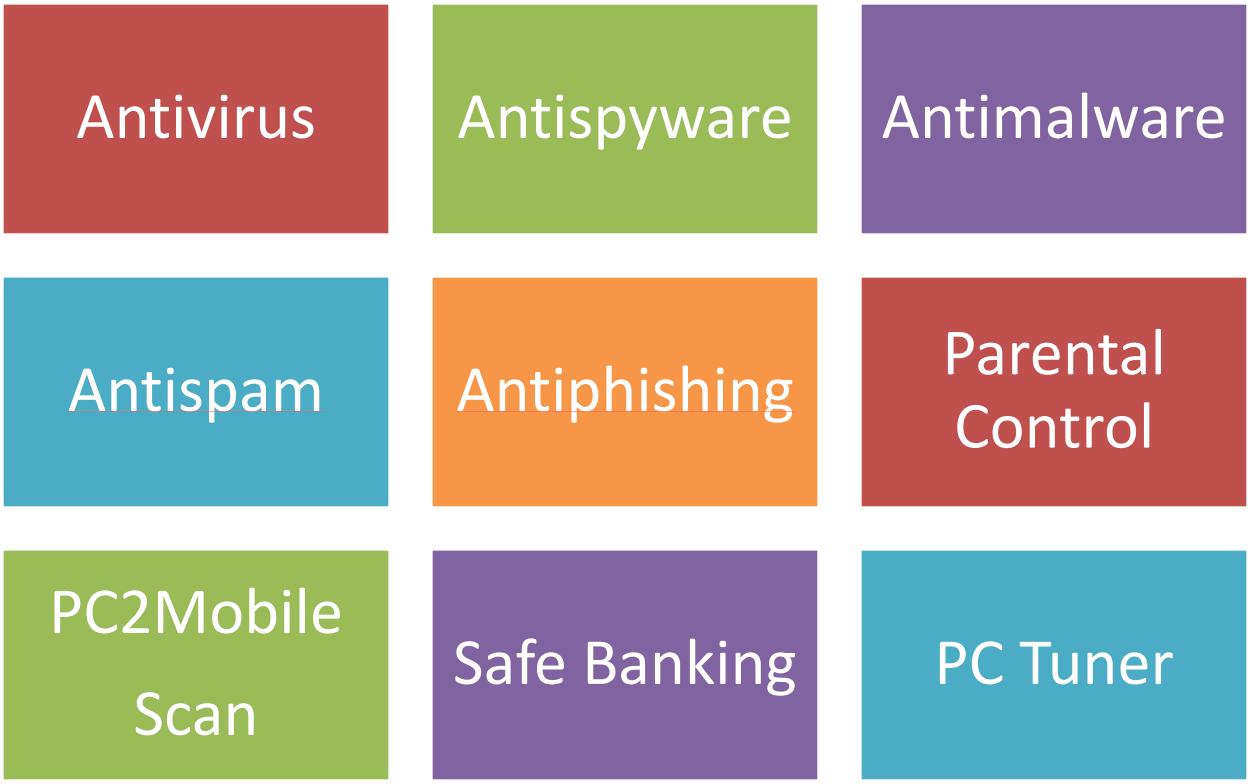


Figure 1.6 Parameters to select an antivirus tool

Among the other bonus features you will find are secure browsers for financial transactions, secure removal of sensitive files, deleting traces of computer and browsing history, credit monitoring, virtual keypad to foil key loggers, cross platform protection and more. Means safe banking must be the additional feature supported by an antivirus tool to be selected.

Today everybody is having mobile phones and we often click the photos wherever we go for outing and to capture the memorable moments in our life through the camera provided in it. Most of the times we transfer the data, images, movies and downloaded files from mobile to our PC to spare the mobile's limited memory. So PC2Mobile scan is must feature to look in for the antivirus tool to be selected.

Take every danger out there for adults on internet and multiply it by kid's naivete and disregard for consequences to get an idea of how much trouble kids can innocently find in digital world. Hence the AV Tool to be selected must have parental control feature which includes inappropriate content filtering for safe surfing, limiting of online activities and even GPS tracking to help keep your kids safe.

In order to stay fully protected, your antivirus must stay up to date on most recent developments because everyday hackers double-up on their efforts to bypass today's powerful antivirus tools.

There are many available choices that provide the very best virus protection. Be sure to consider not only the best price, but what is included in the package as well. Many top antivirus developers offer protection on multiple devices for one price and others may include standout features that offer additional protection. If anybody wants to be fully protected, then selected antivirus tool should support above features so that it will protect your PC against risk on the internet without taking away the freedom to browse on internet, chat and make online purchases without worrying about losing personal information or corrupting system files. Along with one can consider the factors such as budget, operating system, number of devices to be protected, and number of years to be protected.

1.9 Need and significance of study

The expansive number of Anti-virus tools available in the market and some are being propelled and every one of them offers new features for detecting, eradicating and preventing viruses and malwares as compared to the other similar products in the market. Therefore people have a choice of different types of Anti-virus i.e. both in the form of freeware software or licensed software. People much of the time alters their Anti-virus tool as per their liking and needs without accessing the performance and abilities of the various Anti-virus tools available. Subsequently there is a need to discover best Anti-virus software whose performance is best and furthermore suitable for the specific needs of the personal computer users in reasonable price with minimum usage of computer recourses.

Most of the computer users purchase the antivirus tool and they get it installed from the antivirus provider or computer provider. Then they feel that their computer is safe from malwares. The antivirus tool gets updated from internet automatically; it scans the new devices when you connect them. Almost 80% of users keep the default settings of antivirus. They don't even open the settings and try to play around it. It is not possible for antivirus tool to stop all infiltrating malware incidents. It can stop only previously known threats. Once a new threat is recognized it will make new signature available within hours. By the time antivirus company design and deploy the signature for new threat, it offers the sizable window of opportunity for new malware to infect the system due to the absence of security awareness in novice computer users. Most of the new malwares spread due to the misbehavior of new computer user. Signature deployment might also take considerable time; the antivirus servers and networks might not be able to handle updating all of the machines at once. Also, systems that are not connected to the network might not be updated and could become infected (e.g., malware on removable media). The problem of current computer virus defense can be specified like this: Standard anti-virus technology looks for the known viruses when the never-seen-before viruses are actually the ones which cause the problems. It does not matter how quickly the anti-virus vendors respond, their fixes are always reactive. But there should be the proactive efforts from user side also which include user policy, user security awareness, education, operational procedures, controls, review and improvement regarding antivirus tool. Hence the digital hygiene means responsible behavior of the user is efficient mean of cyber protection. Reliance on reactive technology i.e. antivirus tool alone may be a very weak defense against computer virus attack. It should be accompanied with proactive human factor.

Actually human has invented computer to automate manual work. Eventually the invention, growth and usage of internet have changed this digital world giving any sort of information on your desk with a single click and world seems a smaller place with rapid connectivity. In earlier days virus use to spread through floppy disks, USB drives or execution of infected files. But now this interesting ride of the internet seemingly provides is always puzzled with malwares. The real time thriving victims are hooked on

internet. It has become a lucrative business for scammers and fraudsters due to following reasons

1. Rapid growth and daily influx of new and unaware users
2. There are around 3 billion internet users (40% of the World population)
3. Study reveals that 8 new internet users are added every second worldwide which are the 'potential victims'
4. It is easy to maintain anonymity on the internet
5. Fake user accounts, photographs and incorrect location can be easily provided in the online world.
6. 1 out of every 10 profiles across the internet is fake.
7. Every action that needs to be taken can be done from the comforts of home behind the computer screen
8. Knives and pistols are replaced by keyboards and mouse.
9. Internet connection is easily affordable.
10. Email and social profiles are free most of the times and one user can have multiple accounts.
11. Maintaining website is very easy and reasonable

Following are some of the popular scams on internet.

1. Fake ads on online classifieds or auction websites

   In this type of scam, scammer list high value goods such as luxury car at very low prices. They demand some form of processing payment in smooth way to inquiries and once the initial registration money has been paid the fake sellers and scammers stop responding to all emails and calls.

2. LinkedIn Phishing Email Scam

   LinkedIn users reported about receiving emails that seems to be from linkedIn support. The recipient is informed about 'irregular activities' in their account because of which a compulsory security update is required for that user is advised to download an HTML file attached to email. If you click HTML file, it will redirect you to fake website that looks like actual LinkedIn login page and if

you provide login information on this link, it will be directly transmitted to the attacker who will hijack your account.

3. Work From Home Scam

   In this scam mostly unemployed people are targeted in which job posting are placed on social networks, emails and other websites. On clicking the job posting the visitor is directed to a page demanding some amount as registration fee which results in scam.

4. Nigerian Fraud

   It is an organized crime mainly executed via email which consists of 7% of the spam mails worldwide. Victims have lost 12.7 billion dollars globally and Indians top in the victims' list losing $870 million. Victims are assured to get an unbelievably large sum of money and then try to gain trust and send feelers to the victim. On replay victims are asked to pay a sum upfront to facilitate transfer. Once the sum is paid the scammers are out of contact and out of reach.

5. Online Romance Scam

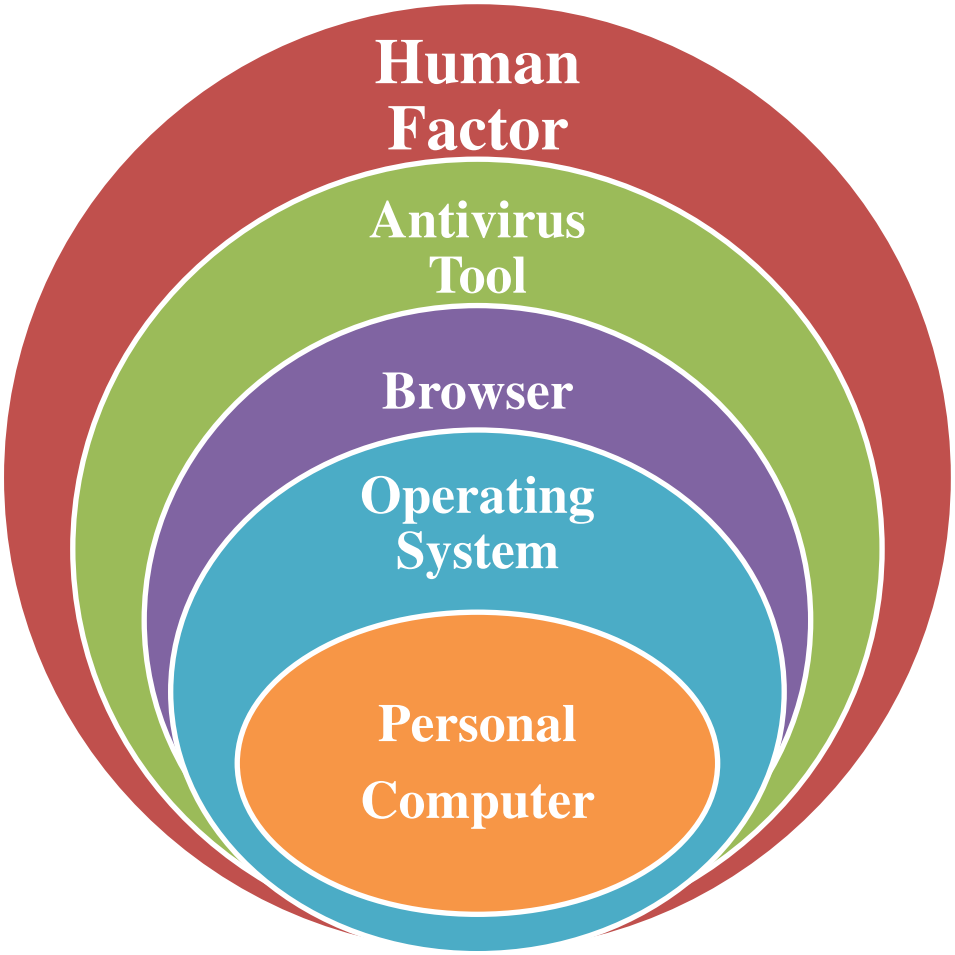
   In this type of scam, scammer plays emotional triggers to get victim shell out of money, gifts or personal details. Scammers target victim by creating fake profiles on internet dating / social media sites. By sharing personal information and giving gifts scammers try to win the trust of victim which may take often months or even years. Once the trust is established, scammers ask victim to pay money for various reasons such as repaying debts/loan, setting up a business. Once they get what they want they will disappear. Which will result in financial loss and victim may suffer from depression and other mental issues.

Antivirus tool will block such kind of attacks and alert you if problems are found. Just usage of antivirus tool is not the complete defense against the computer virus but along with this PC user should increase their knowledge and awareness about internet threats. Also while using AV tool, it should be utilized efficiently and effectively. When PC users are using antivirus tool , the operating system on which the antivirus tool is installed and browser which gets you around the internet are also the factors to be taken into consideration. Because if Av Tool, operating system and browser are fully configured and updated then only they will safeguard the PC from incoming internet threats. To

make an optimum use of antivirus tool you have to configure the settings in antivirus tool, browser and operating system. Most of the times people use the default factory settings provided in it. Here the role of human factor is very crucial. Otherwise it will be an example of house which is having front door locked but back door open for robbers. The antivirus tool is reactive one while there should be proactive contribution from the user side then only your system will be safe otherwise it will provide loop holes for cyber criminals.

To manage an antivirus tool means take the time to create a system that protects them, which, once put in place, doesn't require much time to maintain or upgrade every now and then.

Figure 1.7 Entities involved in Antivirus Tool Management



Hence the researcher is identifying the domain of management of antivirus tool for personal computer security. Through this research, researcher tries to provide keys to PC user which will be used to open the doorways to treasure room of management of antivirus tool towards the security of personal computer.

1.10 Chapter scheme

Researcher has done the following chapter scheme based on study.

No.	**Name**
Chapter No.1	Introduction
Chapter No.2	Review of literature and Conceptual background of virus and Antivirus Tools
Chapter No.3	Research Methodology
Chapter No.4	Analysis and interpretation of data
Chapter No.5	Findings and suggestions
	Bibliography
	Annexure

The first chapter is of Introduction where the researcher has given brief background about the study.

The second chapter is Review of Literature and conceptual background of virus and antivirus tools. It describes the review of the existing available literature on Securities, various Antivirus tools, prevention from virus, overview of antivirus companies considered for study, list of worldwide organizations providing antivirus comparisons and reviews through the rigorous testing in well equipped laboratories etc. Also it portrays conceptual background of virus & Antivirus tools and also focuses on various kind of antivirus tools and presentation methods.

The third chapter describes the research methodology and research design along with the importance, scope, objectives and hypothesis of study undertaken.

The forth chapter presents the analysis of the data in two parts, Part – I Antivirus Users , Part – II Antivirus Vendors deals with the testing of hypothesis.

The fifth chapter summarizes observations, conclusions, findings and suggestions of the present study. Finally bibliography is given at the end.

CHAPTER 2
LITERATURE REVIEW AND CONCEPTUAL BACKGROUND

2.1 Introduction

One of most fundamental step, in any research is to take a review of available literature related to the research subject. A review of literature facilitates the researcher to determine the specialized subject area. A review of literature also gives in depth knowledge related to the subject matter, helps to expose the gaps remained in the available literature, and provides path and guidance. It sometimes gives different perspectives to look at the particular question. It helps to understand the importance, background and the present position related to the subject selected for the research. It provides background of the earlier studies in the similar subject. It also gives a confirmation that the present study has already taken note of what others have done and written in selected area. Therefore, it is necessary to review all kinds of literature related to the subject matter. A review of the work in the computer security domain related to computer virus and antivirus tools is presented.

2.2 Literature Review

1. Computer Virus: Theory and Experiment, Fred Cohen, Computer & security 6, 1987, 22-35

The author of this article Dr. Frederick Cohen is an American computer scientist who is popular as an inventor of most of the widely used computer virus defense techniques. This is one of the milestone paper on “Computer virus”.

In this research article, the author describes a major computer security problem called a virus. Its ability to attach itself to other program and causes them to become virus well. Every program that gets infected may also act as virus and thus the infection grows. As an analogy to a computer virus, consider a biological disease that is 100% infectious. It spreads whenever animals communicate, murders every single contaminated creatures in a flash at given minute and has no recognizable reactions until that moment. In the event that a deferral of even one week is used between the introduction of disease and its effect, it would leave just couple of villages alive and

would positively wipe out the vast majority of current society. In a same manner, if a computer virus of this type could spread through the computers world, it would likely stop most computer use for some period of time and create problem for modern government, financial, business and academic institutions. Speedy propagation of viruses causes widespread damages to computer systems. Also the author states that to secure a system from viral attack, the incoming information flow must be controlled while to protect against information leakage outgoing information flow must be controlled. Basic theoretical results are presented, and the infeasibility of viral defense in large classes of systems is shown. Dr. Cohen demonstrates that there is no algorithm that can perfectly detect all possible viruses. Defensive schemes are presented and several experiments are described. Computer virus study is important research area with potential applications to other fields, that current system offers little or no protection from viral attack. The only safe policy as of this time is isolationism. (Cohen, 1987)

---

2. Computer Viruses: A Management Perspective, MS Olivier, Centre for Advanced Computing and Decision Support [CSIR], 1990

In this article, the author considers measures against computer viruses in a systematic way. The criteria for such steps are effectiveness, cost-efficiency, minimum disruption of normal operations, fast response and integration with general computer security. The computer industry has now become familiarized with the existence of computer viruses. In this paper author describes viruses and, in checklist form, those steps which should be considered by management when dealing with computer viruses. Some companies have introduced policies to minimize the risk while others are still taking it casually.

To deal with the serious problem of computer virus, author suggests that someone in organization should be given responsibility to deal with possible virus infections. All the employees should be educated about viruses. In Contingency plan he also states that budget should be approved for risk management caused by viruses. This paper concludes that Viruses are a fact of life. It is impossible to prevent viruses but the chances of an infection can be reduced by suitable policy. Costs incurred should be in line with the reduction in risk they offer. Viruses should be addressed formally as part of the computer security policy. (Olivier, 1990)

3. Biologically Inspired Defenses against Computer Viruses, Jeffrey O. Kephart, Gregory B. Sorkin, William C. Arnold, David M. Chess, Gerald J. Tesauro, and Steve R. White, Kephart, LSE Research Online, 1998

In this research work, the author describes that today's Anti-virus technology, based largely on analysis of existing viruses by human experts. In a few years, intelligent agents navigating through highly connected networks are likely to form an extremely fruitful medium for a new breed of viruses. First the rate at which the new viruses are created is very fast. And second continued increases in interconnectivity and interoperability among the world's computer users are beneficial to users but also desirable state for fast propagation of computer viruses. To deal with this problem IBM researchers are developing novel, biologically inspired Anti-virus techniques designed to prevent both today's and tomorrow's viruses. Here authors describe two of these: a neural network virus detector that learns to discriminate between infected and uninfected programs, and a computer immune system that identifies new viruses, analyzes them automatically, and uses the results of its analysis to detect and remove all copies of the virus that are present in the system. Here author's hope is that a computer immune system will deal with most of the standard, run-of-the-mill viruses quietly and effectively, leaving just a small percentage of especially problematic viruses for human experts to analyze. (Jeffrey O. Kephart, 1998)

---

4. Computer Crimes: How to Avoid Falling Victim, Dr. John A. Marshall, Journal of Industrial Technology, May 1999 to July 1999

Like food, air and water internet has become the basic need of our life. However this information super highway is rigged with issues. This article provides insights and ―safety instructions designed to prevent Internet users from becoming Internet victims. Internet is an ocean of knowledge. Internet access is becoming an essential requirement in a variety of curriculums. In fact, it is an excellent educational and research tool well suited for many Industrial Technology courses. Surfing the Internet is exciting, valuable, and very informative. While using internet, we should identify potential dangers associated with it. All Internet users should be aware of these types of events and techniques. Educators who encourage Internet use among students may wish to include these precautions in their discussions. The five types of computer crimes presented in

this series represent the types of challenges that face an information society dependent on computers.

1. The first type of computer crime is Deeyenda Plague which is a program that steels sensitive information such as email and login passwords, credit cards, personal information etc. This virus spreads on internet through sending email under the title "Deeyenda" by miscreant. So if anybody get this kind of email, don't download the file.
2. The second type of computer crime is "Man – in –the middle attack" known as spoof, occurs when a user visits a booby-trapped web page. Once visited this site can travel with the user & steal the user information as they access other legitimate. As at prevention the author suggests that when you access any site, carefully type the URL into the browser or add bookmark to the site as soon as browser arrives there. In future only use that bookmark to access the same site.
3. Third crime is browser which allow computer user to surf the net and also hackers and marketers to record the sensitive information of the user through the cookies. So the smart user should empty out the cookies by safely deleting it.
4. The fourth and fifth crime is concerned with stealing the sensitive information such as credit card details, internet passwords.

   The cost and inconveniences caused by these crimes is huge and escalating each day. The insights and safety instructions discussed here have been designed to prevent Internet users from becoming Internet victims. A greater number of hackers are young computer-trained teenagers who don't understand the consequences of using their knowledge for illegal purposes. Taking the time to identify potential dangers should be an integral co mponent in all curriculums. (Marshall, 1999)

---

5. Computer Virus – Technol ogy Tips, Stanley R. Johnson, IOWA State University, PM 1789j , Revised, June 2000

In this research paper, the authors describe information about computer virus, different types of virus. It also describes different sources to get computer virus in to computer system, information about hoaxes and its factors. Also depict the information about Anti-virus software and prevention method of attacking malware (Johnson, 2000)

---

6. Computer viruses: The threat today and the expected future, Xin Li, Avdelning, Institution Division, Department, 2003

The author has submitted this Master's Thesis within the area computer security. Firstly, the definitions of computer virus and the related threats are presented. Secondly, current circumstances of computer viruses are talked about, the working and spreading mechanisms of computer viruses are looked into in depth, and oversimplified attitude of computer world in computer virus combat is investigated. Thirdly, today's influencing factors for near future computer virus epidemics are explained, and then it further predicts new possible types of computer viruses in coming future. Furthermore, currently available anti-virus technologies are broke down concerning both advantages and disadvantages. Finally, new promising trends in computer virus defense are explored in details.

In this research article, the author has described that the virus problem will continue to evolve, just as it has for the past decade or so, and sometimes in unexpected directions. In the beginning most of the viruses spread through the floppy disk. But the explosive growth of the Internet and the rapid emergence of applications that disregard the traditional boundaries between computers threaten to increase the global spread rate of computer viruses by several orders of magnitude. The nature of computer viruses and their ability to propagate is on the cusp of a fundamental, qualitative change -- one that demands an equally fundamental change in the way we must defend against them. We should admit the fact that there is no perfect defense. We should choose active methods which include avoidance, detection and cure, rather than only prevention. It means that system users need to adopt a healthier system 'life style' as well as using the best of 'modern medicine' to avoid catching a virus.

Some good, basic security practices can really help to reduce the risk of computer virus infections, and decrease the cost (and pain) of cleanup after computer virus infection. Some good examples include keeping good clean backups, reviewing security controls on a regular basis, using access controls for system users, limiting connectivity, audit, limiting/controlling media such as diskettes, cd-r/w, zip drives, etc., user awareness and education, risk analysis and reactive and proactive defenses. The new promising immune system is likely to be an important tool to control their spread for the foreseeable future.

Conspicuously author affirms that six technological influencing factors have had a huge impact on the variety and complication of computer viruses and worms: computing infrastructural

homogeneity, ubiquitous programmability, technology migration to home, and increasing connectivity through a homogeneous communication mechanism. Home users, corporations and government entities need to seriously reconsider their security policies, and Anti-virus companies need to start working on the next generation of Anti-virus protection. (Li, 2003)

---

7. Guide to Malware Incident Prevention and Handling, Peter Mell Karen Kent Joseph Nusbaum, National Institute of Standards and Technology, NIST Special Publication, 800-83, 2005

This publication is divided into five sections. Section 1 is the introduction of the topic. Section 2 defines, discusses, and compares the various categories of malware. Section 3 provides recommendations for preventing malware incidents through several layers of controls. Section 4 explains the malware incident response process, focusing on practical strategies for detection, containment, eradication, and recovery in managed and non-managed environments. Likely future developments and trends in malware are highlighted in Section 5.

The guide also contains several appendices with supporting material. This provides recommendations for improving an organization‘s malware incident prevention measures. It also gives useful recommendations for enhancing an organization‘s existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. The recommendations address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools such as backdoors and Rootkits. In this paper authors suggest that antivirus software should be configured and managed properly to continue effective detection and prevention of malware. The recommendations encompass various transmission mechanisms, including network services and removable media. (Peter Mell, 2005)

---

8. Book :Michael Erbschloe, (2005), TROJANS, WORMS, AND SPYWARE A Computer Security Professional‘s Guide to Malicious Code.

This important book provides practical, easy to understand, and readily usable advice to help organizations to increase their security and decrease the possible risks of malicious code attacks. Despite the global downturn, information systems security remains one of the more in-demand professions in the today digital world. With the widespread use of the Internet as a business tool, more emphasis is being placed on information security than ever before. To successfully deal

with this rise in dependence and the ever growing threat of virus and worm attacks, computer users need a jargon-free book that addresses the practical aspects of meeting new security requirements.

This book presents a comprehensive list of threats, an explanation of what they are and how they wreak havoc with systems, as well as a set of rules-to-live-by along with a system to develop procedures and implement security training. It is a daunting task to combat the new generation of computer security threats – new and advanced varwiants of Trojans, as well as spyware (both hardware and software) and "bombs" – and Trojans, Worms, and Spyware will be a handy must-have reference for the computer security professional to battle and prevent financial and operational harm from system attacks. To summaries, this book provides

1. step-by-step instructions to follow in the event of an attack
2. Case studies delineate the "do's," "don'ts," and lessons learned from scandalous attacks
3. computer users the significance of having protocols and a response plan in place (Erbschloe, 2005)

---

9. Anatomy of Computer Viruses, Chuck Hauge, CPH Solutions, 2006

In this research article, the author has described the origin of computer virus and history of computer virus with most dangerous virus and some steps to protect against computer viruses. And also described computer viruses are mysterious and grab our attention. A properly engineered virus can have an amazing effect on the worldwide Internet. He has explained the Viruses - both "traditional" viruses and the newer e-mail viruses and how they work and how to protect your data. Viruses in general are on the wind down, yet sporadically a person finds another way to create one, and that's the point at which they make the news. Author has given three reasons behind the creation of viruses.

1. psychology that drives vandals and arsonists
2. To experience the thrill of watching things blow up
3. To brag rights

Virus creators cause real damage to the computer user due to their creations. So legal system is getting much harsher in punishing the people who create viruses.

To combat against viruses the author gives following suggestions as

1. Start use of secure operating systems like unix or Mac OS
2. Purchase and install antivirus software
3. Avoid the free programs from unknown recourses provided through internet & stick to licensed software
4. Enable Macro virus protection in all Microsoft applications and Microsoft operating system and never run macros in a documents it they are not required
5. Never double click on attachment provided through an email from an unknown recourse (Hauge, 2006)

---

10. Seminar Report on Study of Viruses and Worms, H. Shravan Kumar, Prof. Bernard Menezes, KanwalRekhi School of Information Technology, IIT Bombay, 2006

In this article, authors describe computer virus as a high profile threat to information integrity. Along with computer viruses, computer worms are also increasing day by day. Hence it is necessary to immunize the internet by creating awareness about the internet threats. The authors have explained about different malicious code environments and discussed about the different types of viruses and worms, different characteristics of computer virus and detail about the various ways of virus, worm and their categories, propagation techniques and their differences, it also include case studies of Slammer and Blaster worms. In that case studies author explain how these worms are working. (H. Shravan Kumar & Prof. Bernard Menezes)

---

11. A simple guide to Computer Viruses and other dangerous little programs - An Introduction to an Effective Defense, Roberto Dillon , International journal of law and technology, Program and Play - Roberto Dillon, 2007

In this research article, the author has described information about computer malware, types of malware. Computer malware has been a serious issue for many years and, it‘s very likely to stay with us for a long time to come. There are many tools at our disposal, including excellent free ones, for arranging an effective defense and this will introduce you to the various dangers you might face in future together with easy methods for getting rid of them and restore your

computer an healthy status. Each of the main malware categories are faced one by one by explaining what they do. (Dillon, 2007)

---

12. Protecting Your Computer and Your Identity, Security Awareness, Office of Enterprise Security Dept. of Information Technology, 2007

In this research article, the author has described the importance of protecting our computer and personal identity. If you have a computer connected to the internet then protecting your computer is difficult. Such computer is not only inclined to viruses, spyware and other unwanted traffic including theft of information from your computer, but can also be used by criminal or spamming purposes by hackers. It is common myth that it is not required to protect the computer if it does not contain any important data. This misunderstanding should be removed from computer user's mind because cyber crook can use your computer as scapegoat to launch attacks, commit criminal acts and send out spam. Due to which computer users may be punished for a crime which they have not done. So it is very important to protect your computer and your identity especially when computer is connecting to the web. In this paper author has explained

1. Viruses, Worms, and Trojans

   A virus is a program that can cause damage to the computer and can replicate itself over the network or internet. Virus can corrupt or delete files or make a computer unusable.

   Worm is a self contained program that is able to spread copies of itself to other computers. It does not require the host program but the propagation usually takes through the internet.

   Trojan is a program that looks as benign and neither replicates or copies itself but it allows somebody from a remote site to take control of computer to which it is attached and lead to loss of personal information or identity theft.

2. Spyware is a means of eavesdropping which is installed on computer without user's knowledge or consent by just clicking wrong website. Most spyware come from free programs that we download from internet. It also cause browser hijacking which changes home page of your browser. For example if you are planning a Goa vacation then you may be surprised to see relevant ads on travel deals to Goa as pop ups, emails or other messages. If computer is infected with spyware then your online activities are recorded

and you will be targeted for ads. It runs in background and slows down the overall performance of a computer. Spyware requires specific antispyware tool to identify and remove it.

3. Spam is unrequested email sent in large quantity for advertising or marketing on the internet. Spammers collect email addresses from various sources and ask the user to click a link to unsubscribe from their email list which results to confirm your email id and cause more spam to be sent.
4. Phishing is a criminal activity attempting to fraudulently acquire sensitive information such as passwords or credit card details by pretending as a authentic person or a business. Phishing can be done using email or instant message or through phone contact.
5. Pharming is a word play on farming and phishing used to theft personal credentials. It as a hacker's attack used to redirect website traffic to another bogus website. It can be done by either changing the host file on a pawn computer or by exploitation of vulnerability in DNS server software. It has become a major threat for business hosting ecommerce and online banking websites.
6. Internet Frauds and Scams are initiated by a lot of fraudulent companies and individuals using the internet as a way to lure and scam people. These include "Get Rich Quick" schemes, online auctions, Nigeria email scam, charity and disaster related scams, medical scams and credit card fraud.
7. Online Predators are serious epidemics to the children online. It has been observed that out of four children one child receives sexual solicitation in a chat room.So it an important to understand and monitor the children's online activities is an issue needs to be addressed.
8. Cyber Bullying is an use of electronic medium to bully a person by verbal harassment of an intimidating or threatening nature.
9. Identity Theft is a fastest growing crime on the internet which steals victims personal information which will cause the victim months or even years to recover from and can cost those person very much. They could lose job opportunities, be refused loans and even be arrested for crime even though they are innocent. This is an emerging serious issue on internet and needs to be addressed.

   Tips to protect your computer and identity :

a. Install antivirus
b. Install a firewall with combination of hardware and software firewall to have well protected system
c. Update windows and browser regularly
d. Keep browser security at medium or high
e. Increase security settings in windows
f. To control spyware
    i. Install antispyware tool
    ii. Don't install "search help bars" in browser
    iii. Don't run executable attachments even if it is sent by a friend
    iv. Limit who you give your email address to
    v. Don't respond to any spam
    vi. Report spam and make use of good spam blocker
g. To avoid phishing
    i. Never give out personal or financial information in response to unsolicited emails
    ii. Be able to recognize a phishing attempt
    iii. Check your credit card and bank statements on regular basis
    iv. Report phishing attacks immediately if any
h. To control pharming
    i. Pay careful attention to the spelling of the address
    ii. Check the website's certificate
    iii. Look for padlock or key at the bottom of browser
    iv. Always be careful with your personal information
i. Tips for online predators containment
    i. Keep user names and profiles generic and anonymous
    ii. Promote healthy internet habits among your child
    iii. Place the personal computer in an open area
    iv. Respect children's privacy
    v. Educate your child about the online predators
j. Tips to avoid cyber bullying

i. Educate your children on the danger of cyber bullying
ii. Don't open or read any messages from a cyber bully
iii. Don't respond to the cyber bully with anger
iv. Save the evidence and report cyber bullying
v. Report any type of threat to law enforcement immediately

k. Tips to protect your identity
i. Monitor your bank account regularly
ii. Always careful when you provide your information online
iii. Don't respond to unsolicited emails, links or pop-up ads
iv. Shred all documents that plan to throw away
v. Try not to keep too many credit cards if you don't use them regularly
vi. Protect and store personal information at home
vii. Protect your mail
viii. Beware of "shoulder surfers"
ix. Place a fraud alert on your credit (Protecting Your Computer and Your Identity, Security Awareness, Office of Enterprise Security, 2007)

---

13. Computer Virus Preventing and Controlling Method Discussion, ShenYanmei1, XieHong, Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (ISECS '10), July 2010

This article provides a brief introduction of the computer virus concept and it's characteristic and has listed some computer virus typical symptoms. It introduced the computer virus treatment method through the example. Some virus even can format the hard disk or make the hard disk impossible to use. Virus biggest harm is enabling the entire network to sink into the paralysis. In the near future, the computer virus is spreading seriously, these virus is trying to close each kind of Anti-virus software and automatically download dozens kind of robber number wooden horse virus, and will bring the major loss to the user. To detect and remove this virus is more difficult than— the panda to burn incense. So, computer virus preventing and controlling work appeared especially important for safe use of computer. (XieHong, 2010)

---

14. Computer Viruses as a Threat to Home Users, Dr. Waqar Ahmad, International Journal of Electrical & Computer Sciences IJECS, 2010

In this research article, the author has described the growth of Computer virus threat and home users are threatened by them, especially with the rapid increasing dependence on computers to accomplish the vast verity of tasks in our modern lives. The use of internet can be easy and fun. Any sort of information is easily available and world seems to be smaller place with the connectivity but it provides the ideal environment for virus writers. This paper describes definition of computer viruses, their nature, their history and development, and their different types. The virus is structured as search routine, copy routine, anti detection routine and payload routine. Virus life cycle comprises of the stages as birth, release, proliferation, trigger, activation, detection, elimination, modification. The virus types are outlined as file infecting virus, macro virus, script virus, and polymorphic virus.

In today's digital life the computer has become integral part of every individual's life. In modern home nowadays computer has same importance as TV and telephone. All the members of family use the computer for different tasks depending upon their needs. All the members belong to different age groups, different position and different computing knowledge sharing the same home PC. Hence the technology interference in our life has made us more dependent on computer and internet. But the computer virus is the most common peril which attacks the computer functionality and reliability. Since the computer users in the family vary in their computer knowledge they may be prayed as victims by hackers. Day by day the home users are increasing making computer virus more hazardous. Hence this is critical issue and needs to be addressed.

Author has analyzed the computer virus writer's types as adolescent (age between 13 to 17), college students(age between18 to 24), adult/professionally employed and Ex-virus writers which belongs to different age group and educational level. Author reveals the fact that these virus writers could be motivated by the need to express their dissatisfaction with their social level, draw attention, make fame, achieve their revenge with society or want to prove their technical knowledge.

Since the computer virus is serious issue increasing day by day throughout the world to mitigate it's effect most of the countries around the world have applied legislation laws for computer crimes and some of the virus writers got caught and are paying out their sentence.

Dr. Waqar Ahmad appeal that to fight with computer virus threat home user should increase their knowledge about computer viruses, antivirus software, firewalls. He demonstrates this with example of home owner who get robbed if he kept front door open will not get any sympathy. In a similar manner if home user keeps his/her computer open to the intruders or hackers will be blamed for his/her carelessness. So every home computer users should increase their knowledge and awareness about the computer security is the best solution to combat with computer virus. (Ahmad, 2010)

---

15. An Analysis of Information Security Awareness within Home and Work Environments, Shuhaili Talib, Nathan L. Clarke and Steven M. Furnell Centre for Security, Communications and Network Research (CSCAN), University of Plymouth, Plymouth, PL4 8AA, United Kingdom

In this research paper, the authors have analyzed information security awareness within home and work environment using survey method. The aims that are examined in survey are

1. To understand respondents general levels of security awareness and practice.
2. To understand whether they received training from work and if so, what type and how effective it was.
3. To understand the relationship between knowledge gained and practice between work and home
4. To understand how people learn and what preferences they have towards various learning styles

Authors propose that attaining information security awareness in the general population of computer users using internet is essential if they want to stay safe. According to researchers, security awareness education requires combination of time, recourses and motivation. Comparison of work and home environment proves that later provides more opportunity. Transfer of knowledge from workplace to home is in progress. (Shuhaili Talib)

---

16 .How Computer Viruses Work, Marshall Brain, Manitoba E-Association's, How stuff work, 2010

In this article, the author has elaborated about viruses -- both "traditional" viruses and the newer e-mail viruses. Article also explains how they work and also understand how to protect yourself. Viruses in general are on the wane, but infrequently a person finds a new way to create one, and that's when they make the rumor. And also he has explained the most common infection types. Like virus, worms, Trojan. Working and prevention method of cold red and I love you virus are discussed. (Fenlon, 2010)

---

17. An Overview of Computer Viruses in a Research Environment, Matt Bishop, the Dartmouth Computer Science Research Symposium (CSRS2011), 2011

In this research article, the author has described the threats that computer viruses cause to research and development multi-user computer systems. It has attempted to tie those programs with other, usually simpler, programs that can have equally destructive effects. Although reports of malicious programs in general adhere, no non-experimental computer viruses have been reported on mainframe systems. This paper has described several easily harmed methods in the research and development environment that malicious programs could exploit, and also discussed research current in progress to improve defenses against malicious logic. Noting that the number of people with access to mainframes is relatively small compared to the number with access to personal computers. Should an attacker use a computer virus or other malicious program, security mechanisms currently in use will be as effective as they are against other types of attacks. (Bishop, 2011)

---

18. Malware Threats and Mitigation Strategies: A Survey, RizwanRehman, Dr. G.C. Hazarika, GunadeepChetia, Journal of Theoretical and Applied Information Technology, 2011

In this paper, the authors have focused on the growth in E-commerce, today‘s open source nature of malware, the growing penetration of the Internet in respect to insecure connected PCs, are among the main targets of the scene. It discusses different trends and techniques used for developing malware and a survey on how these can be handled in an efficient manner. It also discussed about various issues related to malware beginning first from the structural properties of the malware and its conduct which is necessary for analysis so as to able to defend them. At the

end author discussed about the latest mitigation strategies which can detect the malware, latest techniques which are being used for the mitigation which are classified as signature based detection, host based detection, firewall and malware defenses, proxy based defenses. It further proposes the usage of virtual environment within network device since these malware applies various methods to hide and obscure them. This will promote the security device to test malware behavior in safe environment without causing harm to host program or operating system. (Rizwan Rehman, 2011)

---

19. Cybersecurity for Dummies , A Wiley Brand, Palo Alto Networks 2nd edition, by Lawrence C. Miller, CISSP

This book describes how advanced threats have changed the world of enterprise security and how organizations are attacked. These threats, and the cybercriminals behind them, are specialists at staying hidden from conventional security while exhibiting an intelligence, resiliency, and persistence that have never been seen.. Controlling these threats requires multiple security disciplines working together in context. Although no single solution will solve the problem of advanced threats on its own, next generation cyber security provides the unique visibility and control of, and the true integration of, threat prevention disciplines needed to find and stop these threats — both known and unknown. (Miller)

---

20. A Brief History of Antivirus Software, techlineinfo.com

This article presents the history of antivirus software. One of the first major outbreaks of a computer virus was named *Brain* and with it the antivirus industry is started. Early computer viruses rarely had malicious intent. Eventually, as the techniques began to spread, these intentions turned toward bad intent. By 1987 there were two antivirus utilities available as Flushot Plus and Anti4us. Between 1987 and 1989, a group called "Virus-L" was being used to update individuals about security and sharing information, tools, and shareware to assist to remove the virus infection. Two individuals on this list were John McAfee and Eugene Kaspersky. In 1989 John McAfee went on to start his own business selling software that protects both hardware and software. Other software brands, such as Kaspersky and Norton, were introduced to the market

with success. However, security holes in earlier versions of operating systems we've all come to know and love were very prevalent. The lack of communication resulted in major losses as computers became increasingly adopted in business and at home.

Handling computer viruses and malicious attacks were difficult enough on a closed system. It was pure hell once everyone became connected through an online connection. The ability to send email, download programs, and run coded scripts gave hackers the opportunity to infect and steal data from anywhere in the world without needing physical access to systems. Unknowing users were and still are often the ones who aid in the spread of these viruses.

With the changing landscape of distribution, antivirus software began to make advancements in detections and gained the ability to update itself online, which improved effectiveness.

Eventually, the introduction of the web also allowed for an expansion into cloud-based antivirus, network firewalls, online scanning, and specialty tools aimed at removing specific files and issues with a computer or network. (TechLineInfo, 2013)

---

21. A Comparative Study for Performance Measurement of Selected Security Tools, International Journal of Engineering Science and Technology Vol. 2(10), 2010, 5130-5136

Mr. Bhaskar.V. Patil, Dr. Prof. Milind. J. Joshi, Mr. Hanmant. N. Renushe

Explosive growth in use of internet results in new flexible opportunities also measure security threats poses in the networks. These threats can external or Internal, external threats divided as hacking, virus attack, Trojans, worms etc. This paper presents the detailed study on types of virus. These all types of malwares can be contained by usage of antivirus tools. There are number of network security tools and antivirus tools are available in market. But all are not equally compatible for each type of attack. So the selection of antivirus tool is an issue needs to be addressed. This research paper highlights the performance of antivirus software using the number of variables such as installation time, size, memory utilized, boot time, user interface launch time and full system scan time etc. The security tools selected were classified into three categories such as Total Security, Internet Security and Anti-virus Product. Antivirus products provides basic detection and remediation of viruses and spyware. Internet security products provide antivirus tools features along with greater internet protection against phishing, root kit detection, firewall and scanning of web pages and http data.. While total security provides data migration and

backup facility on top of all security features common to internet security products. Each security tool was installed on a computer with Windows XP SP2 operating system, and then tested with the parameters and observations have been registered. The observations are with different units and they need to be converted into Score Point, a unique scale. After that a comparison of performance of each tool is studied using like art-scale method. From the findings of the study, it is observed that four out of thirteen tools belongs to Good Category and remaining nine security tools falls within Very good Category. (Mr. Bhaskar Patil, 2010)

---

22. Commercial antivirus software effectiveness : An empirical study, 0018-9162/11/$26.00 © 2011 IEEE Published by the IEEE Computer Society March 2011 OrathaiSukwong, Hyong S. Kim, and James C. Hoe, Carnegie Mellon University

Most users depend upon antivirus software to keep their computers free of malware, or malicious software. Desirable AV software should accurately identify and stop malware as soon as it enters a computer. Otherwise, it should at least effectively mitigate damages due to undetected malware's execution—for example, taking over the system, creating additional security breaches, or bringing in other malware.

An empirical study conducted to compare the effectiveness of current AV software offerings against malware quantified the fraction of malware successfully detected during the study period and the time required to do so. The study also recorded the software's responses to malware's execution. The empirical results suggest that, despite behavior- based detection, AV software can't effectively detect all current forms of malware. Nonetheless, behavior- based detection raises the bar for system protection. In this process the antivirus tool is technical part but the role of human factor is very important. The hackers are mainly taking the advantage of human behavior. User awareness, education and security policy and operational procedures are also important key aspects to strengthen our fight against cyber security threats. To minimize the risk of receiving malware, users must take precautions before downloading or opening any unknown files and, obviously, avoid opening e-mail from strangers. Also authors appeal that it's essential to keep systems up to date. Not all malware blocking software offerings will provide 100 percent Protection, but staying on top of the latest updates certainly can't harm the computer system. (Orathai Sukwong, 2011)

23. Computer Viruses for Dummies, Author: Peter Gregory, CISSP, CISA, Publisher: Wiley ISBN: 0-7645-7418-3, Aug 2004

This book is about computer security for the personal user. Part I of the book deals with assessing the risks that arise when a computer is connected to the Internet and describes how to combat them. The section begins with an explanation of viruses and other malware the computer user may encounter. Next, a general chapter depicts what symptoms and changes a computer may show if malicious code is running on it. These are followed by an introduction to finding, running and updating anti-virus solutions.

Part II is wholly describes anti-virus software. It explains in detail how to evaluate, acquire and install anti-virus solutions. As part of the section on evaluating anti-virus products the book focuses on many functions of the anti-virus software. The next chapter looks at and explains some of the slang involved in configuring anti-virus software. This is followed by a section that is best described as 'what to scan and when to scan it'. Finally, a chapter describes what to do if the software detects a virus. Importantly, this section advises the reader to find out what the virus has done before evacuating it.

Part III deals with the aspects of security software that are frequently ignored. Computer security is not like forestry where you plant a sapling and abandon it - it is more like bonsai, where steady nurturing is required. This includes updating anti-virus data and programs, patching the operating system and applications, and running anti-spyware and firewall programs.

A chapter is devoted to PDAs and describes how they should be protected. Part III finishes with an overarching chapter on how to practice 'safe hex' - from using legitimate software to avoiding spam.

In my opinion Part IV explains how viruses infect and virus taxonomy, which includes further interesting assertions such as: 'The other name for a macro virus is Trojan horse [*sic*].'

Part V, the omnipresent ‘part of tens’, finishes the book. There are two chapters here; the principle concerns virus myths and the second concerns anti-virus programs. The virus myths

range from ‘anti-virus companies write viruses’ to ‘viruses broke my computer’. The last chapter lists ten anti-virus programs with a two-third page summary which lists manufacturer, website etc., along with a ‘yes/no’ list of features. (Gregory, 2004)

2.3 Overview of worldwide organizations providing antivirus comparisons and reviews

1. www.pcmag.com

Pc Magazine is site which provides answer to all questions related to computers and software that runs on them, including antivirus. To access the reviews, type “best antivirus” in the search box and choose one of the two top articles by Neil Rubenking (one of the top experts in the field). In review you will notice available price and few conclusions. Here you can evaluate the performance based on malware blocking, malicious URL blocking, phishing detection, privacy detection and additional features. This sites provides you the guidelines for the selection of antivirus tool. (PC Magazine)

---

2. www.av-test.org.

It is German laboratories in Magdeburg comprising of 30 IT specialists boasting many years of expertise take a practical approach to the development of innovative analysis mechanisms and the application of high-quality test procedures. In order to achieve these objectives, AV-TEST provides optimal working conditions and development opportunities. After all, IT security is one of the key factors in the modern business and corporate world!

The AV-TEST Institute is a leading international and independent service provider in the fields of IT security and anti-virus research. The aim of the research work carried out by AV-TEST is to directly detect the latest malware, to analyze it using state-of-the-art methods and to inform computer users about the top-quality results obtained. AV-TEST uses three criteria to judge antivirus tools as protection, performance and usability for mobile, home and corporate users. An antivirus can obtain maximum of 6 points for each criteria. Under protection criteria protection against malware infections such as zero-day malware attacks, web and email threats are checked. Performance measures the impact of antivirus tool on PC’s speed and general performance.

Usability recapitulates impact of antivirus tool on the usability of the whole computer. In order to process large quantities of data, AV-TEST has set up high-quality and efficient technical research environment Managing Over 1,500 Terabytes of Test Data. (Av Test Independent It Security Institute)

---

3. www.av-Comparatives..org

“We put the most prevalent anti-malware software through our comprehensive, impartial and realistic testing environments to prove that they truly protect against threats. Our outcomes furnish consumers with an independent rating so they can compare various products on the market and use the appropriate solution for their requirements." Andreas Clementi, Chairman of AV-Comparatives

AV-Comparatives is located in Innsbruck Austria and is an independent organization offering systematic testing that checks whether security software, such as PC/Mac-based antivirus products and mobile security solutions, lives up to its promises. Using one of the largest sample collections worldwide, it creates a real-world environment for truly accurate testing. AV-Comparatives offer freely accessible results to individuals, news organizations and scientific institutions. Certification by AV-Comparatives provides an official seal of approval for software performance which is globally recognized.

At present, AV-Comparatives' Real-World Protection Test is the most exhaustive and complex test available when it comes to accessing the real-life protection capabilities of antivirus software. Put simply, the test framework duplicates the scenario of an everyday user in an everyday online environment – the typical situation that most of us experience when using a computer with an Internet connection.

AV-Comparatives works closely with several academic institutions, especially the University of Innsbruck’s Department of Computer Science, to provide scientific testing methods. Further it propose that, if you plan to buy an Anti-Virus, please visit the vendor's site and evaluate their software by downloading a trial version, as there are also many other features and important things for an Anti-Virus that you should evaluate by yourself. Even if quite important, the data

provided in the test reports on this site are just some aspects that you should consider when buying Anti-Virus software. (Av Comparatives)

---

4. www.virusbulletin.com

An requisite source of reference for anyone concerned with computer security, the Bulletin is the forum through which leading security researchers publish the latest security research and information in a bid to share knowledge with the security community. Publications cover the latest threats, new developments and techniques in the security landscape, opinions from respected members of the industry, and more. The Bulletin archives offer informative articles going back to 1989.

With almost two decades of experience, VB is one of the world leaders in security software testing. It provides comparatives which cover anti-malware protections of all types as well as enterprise-level email and web security solutions. Their team of expert testers and testing frameworks are also available for a wide range of private testing and consultancy work.

A world-renowned security event, the annual VB Conference has been running for over 25 years, covering a broad range of IT security topics and providing a venue for the brains of IT security from around the world to learn, debate, pass on their knowledge and move the industry forward. The VB Conference is considered by many to be a must-attend security event.

In short, Virus Bulletin is an important benchmarking and comparison site for the entire antivirus industry. It measures just about everything you can think of, including install times, scan speed, stability, performance impact, false positives, detection rate and so on. (Virus Bulletin)

2.4 Antivirus tools products overview of selected companies

In the current study the researcher has selected following company's antivirus tools for the performance measurement which are the results of pilot study. The selection criteria applied is the number of users is selected from pune city.

AVG Antivirus

www.avg.com

AVG - Dedicated to online security. AVG products protect devices, data, and people. AVG antivirus is security pioneer, offering a wide range of protection, performance and privacy solutions for consumers and businesses. AVG is now part of Avast family of world leading digital security products, dedicated to keeping people around the world safe.

For personal computers installed windows operating system, AVG provides following products

- AVG Ultimate for unlimited devices provides
  - ❖ Advanced antivirus & tuneup package
  - ❖ Secure & tune up all your PCs from one screen
  - ❖ Live phone or chat support
  - ❖ Real-time security updates
  - ❖ Automatic tuning updates
  - ❖ Includes Mac & Android apps
  - ❖ Unlimited installations
- AVG Internet Security for Unlimited Devices
  - ❖ Stop viruses, spyware, & other malware
  - ❖ Block unsafe links, downloads, & email attachments
  - ❖ Get real-time security updates
  - ❖ Encrypt & hide your private photos & data
  - ❖ Detect fake websites for safer payments
  - ❖ Includes phone and chat support
  - ❖ Includes unlimited AntiVirus PRO for Android
- AVG TuneUp Unlimited Devices
  - ❖ Advanced cleaning & speed
  - ❖ Duplicate Finder
  - ❖ Remote tuning from one screen
  - ❖ Automatic tuning updates
  - ❖ Live phone or chat support
  - ❖ Includes Mac & Android apps

- AVG Driver Updater
    - ❖ Helps fix device issues
    - ❖ Helps reduce crashing & freezing
    - ❖ Scans for over 127,000 drivers (AVG Antivirus)

Quick Heal Antivirus

www.quickheal.co.in

20 Years of Quick Heal Security

Quick Heal Technologies Ltd. (Formerly Known as Quick Heal Technologies Pvt. Ltd.) is one of the leading IT security solutions company. Each Quick Heal product is designed to simplify IT security management across the length and depth of devices and on multiple platforms. They are customized to suit consumers, small businesses, Government establishments and corporate houses.

Over a span of 20 years the company's R&D has focused on computer and network security solutions. The current portfolio of cloud-based security and advanced machine learning enabled solutions stop threats, attacks and malicious traffic before it strikes. This considerably reduces the system resource usage. The security solutions are indigenously developed in India. Quick Heal Antivirus Solutions, Quick Heal Scan Engine and the entire range of Quick Heal products are proprietary items of Quick Heal Technologies Ltd. (Formerly Known as Quick Heal Technologies Pvt. Ltd.)

For home users with windows operating system it provides following 3 products

- Quick Heal Antivirus Pro
- Quick Heal Internet Security
- Quick Heal Total Security is recognized as 'Top Product' by AV TEST

Product wise comparison is presented in following table (Quick Heal Antivirus)

			
FEATURES	**Antivirus Pro**	**Internet Security**	**Total Security**
Advanced DNAScan	✔	✔	✔
Core Protection			
• AntiVirus • AntiSpyware • AntiMalware • AntiRootkit • Firewall • Intrusion Detection • Intrusion Prevention	✔	✔	✔
Vulnerability Scan		✔	✔
Mail Protection			
• Spam Protection		✔	✔
Internet Protection			
• Browser Sandbox	✔	✔	✔
• Safe Banking		✔	✔
• Phishing Protection		✔	✔
• Web Security	✔	✔	✔
• Parental Control		✔	✔
Privacy Protection			
• Data Theft Protection			✔
• Secure Delete			✔
Anti-Keylogger	✔	✔	✔
Virtual Keyboard		✔	✔

PC Optimization			
• Registry Cleanup • Disk Cleanup • Traces Cleanup • Registry Defragmenter • Duplicate File Finder			✔
Mobile Phone Protection			
• PC2Mobile Scan			✔

Table : 2.1 Specifications of Quick Heal products

For home users Quick Heal provides

Quick Heal PCTuner 3.0 which provides following facilities

- Gets rid of junk files from your PC
- Deletes traces of mostly used applications in the system
- Removes unwanted programs from startup
- Deletes files securely so that they remain unrecoverable

Kaspersky Antivirus

www.kaspersky.co.in

"We believe that everyone has the right to be free of cybersecurity fears."

- Eugene Kaspersky *Chairman and CEO of Kaspersky Lab*

For nearly 20 years, Kaspersky Lab has been a recognized expert in the fight against malware and cybercrime. In 2015 alone, Kaspersky products participated in 94 independents tests & reviews and were awarded 60 first places & 77 top-three finishes. Each year, it's share of first

places increases, demonstrating focus on constantly enhancing and improving Kaspersky products. Here comparison of Kaspersky products for home users is provided. (Kaspersky Lab)

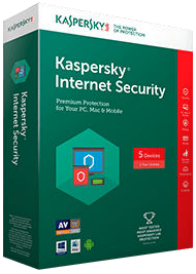
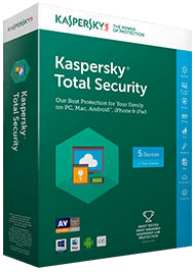
Features	Kaspersky Antivirus	Kaspersky Internet Security	Kaspersky Total Security
			
Security Award wining protection	✔	✔	✔
Performance Optimized security that won't slow you down	✔	✔	✔
Simplicity	✔	✔	✔
Easy to manage security with online access		✔	✔
Privacy Identity protection and more		✔	✔
Money Extra security for online banking and shopping		✔	✔
Parental Control Protection for kids on PCS & MAC Computers		✔	✔
Kids Extended protection for kids on PC, MAC & Mobile			✔
Password Secure storage plus easy access from multiple devices			✔
Files Encryption & backup of your photos, music & memories			✔

Table 2.2 : Specifications of Kaspersky products

Mcafee Antivirus

www.mcafee.com

McAfee is now part of Intel Security. Delivering proactive and proven security solutions and services that help secure systems and networks around the world, Intel Security protects consumers and businesses of all sizes from the latest malware and emerging online threats. Mcafee solutions are designed to work together, integrating anti-malware, antispyware, and antivirus software with security management features that deliver unsurpassed real-time visibility and analytics, reduce risk, ensure compliance, improve Internet security, and help businesses achieve operational efficiencies. (Mcafee Antivirus)

For personal computer users using windows operating system Mcafee provides following products

- Mcafee antivirus plus
- Mcafee Internet Security
- Mcafee Total Protection

The product wise comparison is as follows.

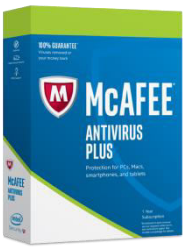
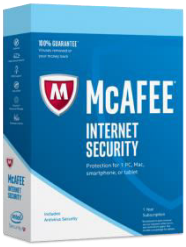
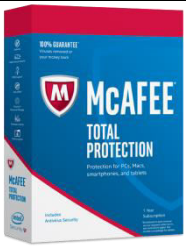
Features	Mcafee Antivirus Plus	Mcafee Internet Security	Mcafee Total Security
			
Protect your privacy with encryption software			✔
Keep your kids safe with parental controls		✔	✔
Block annoying and dangerous emails with Anti-SPAM		✔	✔
Eliminate the hassle of passwords, let the True Key™ app remember them for you - See more at:		✔	✔
Safeguards your identity and online transactions	✔	✔	✔
Protect all your PCs, Macs, smartphones, and tablets† with the same subscription at no extra cost -	✔	✔	✔
Permanently delete sensitive digital files	✔	✔	✔
FREE Support for the life of your subscription	✔	✔	✔
Includes our 100% Guarantee: Viruses removed or your money back	✔	✔	✔
Avoid risky websites and prevent dangerous downloads	✔	✔	✔
Defends against viruses, malware, ransomware, and other online threats -	✔	✔	✔

Table 2.3 Specifications of Mcafee products

Norton Antivirus

www.in.norton.com

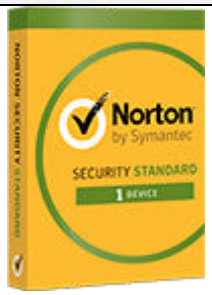
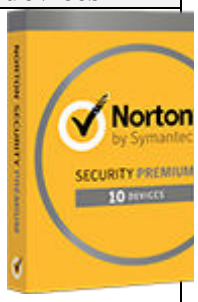
Norton has one of the largest civilian teams of security experts in the world. Noton Security Technology and Response (STAR) team is made up of 550 security engineers, virus hunters, threat analysts and researchers who battle on the frontline of digital crime, continuously monitoring and analyzing new threats — and devising new ways to protect computer user from them.

Over the past 25 years, the Norton team has built a rich proprietary database of security intelligence and one of the largest cybercrime-prevention operations in the world. Attack attempts on any of our 43 million customers provide new data and protection ideas for the STAR team.

Working from nine response centers located across the globe, STAR delivers around-the-clock protection to Norton Security customers, 365 days a year. (Norton Antivirus)

Norton provides following products for windows or MAC PCS

- Norton Security standard for 1 PC or MAC
- Norton Security Deluxe for Up to 5 PCs, Macs, smartphones or tablets
- Norton Security Premium Up to 10 PCs, Macs, smartphones or tablets

Features	Norton Security Standard for PC or Mac	Norton Security Deluxe for for 5 Devices	Norton Security Premium for 10 devices
			
Defends against viruses, spyware, malware, phishing, software vulnerabilities, and other online threats.	✔	✔	✔
Safeguards your identity and online transactions.	✔	✔	✔
#1-ranked consumer security software for overall protection and performance. Protects better and faster than the competition.	✔	✔	✔
Helps ensure that email or links actually came from a trusted source, such as your bank and hospital.	✔	✔	✔
100% guarantee: from the moment you subscribe, a Norton expert is available to help keep your devices virus-free, or give you a refund	✔	✔	✔
Alerts you about risky Android apps before you download them, with our award-winning technology.[1]	✔	✔	✔
Secures multiple PCs, Macs, smartphones and tablets with a single subscription.	✔	✔	✔
Helps you manage protection for all your devices with an easy-to-use web	✔	✔	✔

portal.			
Protects your kids from unsafe content and guards against over sharing online.	✔		✔
Helps you manage and balance your kids' time online and offline.	✔		✔
Automatically backs up your photos, financial files, and other personal information on your PC.	✔		✔
Includes 25 GB of secure cloud PC storage with the option to add more, providing additional protection against ransomware.			

Table 2.4 : Specifications of Norton products

Netprotector Antivirus

http://www.indiaantivirus.com

Net Protector is one of the leading providers of Anti-Virus and Internet Security tools. NPAV was established in India and has been actively involved in Research and Development of Anti-Virus software with motive is to "Add confidence to computing" by developing innovative solution for large corporate, small enterprise and individual users.

Net Protector AntiVirus. Product is popular due to its reasonable and affordable price.

Net protector provides following products for single PC

- **Net Protector Total Security**

Net Protector AntiVirus incorporates a very strong Anti-Virus and Internet Security to defend your Home PC from all cyber attacks and threats.

- **PC Optimizer 2.0**

  Today PC's get cluttered with more damaging data, junk, and extra files than ever. This results in poor PC performance, frequent system crashes, slow Internet connections and worse. PC Optimizer makes your PC fast and stable also removes errors in your windows registry.
- **Web Secure**

Internet is the life-line of all human activities like work, education, business, entertainment etc. But it is important to control and secure the internet and block out the unwanted sites. Keep your Office / Home Secure with Web Secure. (Net Protector Total Security)

2.5 Articles/papers based on features provided by antivirus tools

In this section researcher is describing the papers related to the special features providing best damage control by antivirus companies to combat with the evolving nature of malwares.

2.5.1 Browser Sanbox Protection

Figure 2.1 Browser Sanbox Protection	**Browser**
	is a software application for retrieving, presenting and accessing information resources from World Wide Web. Popular web browsers include Firefox, Internet Explorer, Google Chrome, Opera and Safari. We can access any website by typing it's URL in address bar of browser window.

Nowadays you cannot really tell if a website is clean or puzzled with malicious codes. Only visiting a website can automatically drop a malicious code in your PC. This can happen for trusted, legitimate websites used by hackers to target unaware users.

This can be effectively dealt with proactive security features such as a browser sandboxing which creates a virtual environment and executes your internet browser within this environment inside your PC. Any file that you download or gets downloaded from the browser, remains isolated in the sandbox environment. So, even if any infection does take place from the download, it will remain confined inside the virtual environment without affecting the real PC. And once you close the browser, any changes that

Figure 2.2 Browser Sanbox

might have occurred in the environment will be deleted. This way your actual PC remains unaffected. Nowadays all popular antivirus tools support this feature through which you can control browser access to your personal data on the computer. (Browser Sandbox)

2.5.2 Password Pains

 **Figure 2.3 Remembering Password**	Computer password is an unspaced sequence of characters containing digits, alphabets and special characters used to gain access to computer, web page, network resource or data.

In today's digitized world, every person is having minimum 5 different password for email facebook and banking accounts and to remember these passwords is burden for computer user.

Recent surveys show how widespread the problem has become:

- 33 percent of users have more than ten passwords.
- 25 percent forget three or more passwords every month.
- 30 percent use a smartphone to access online accounts.
- Nearly 40% of users write down their passwords.

But these traditional solutions may prove too risky.

So how do you cope? The methods commonly used are difficult and often ineffective and risky. You can:

- Try to remember them. But with so many different passwords, it's impossible.
- Write them down. Notes with passwords can fall into the wrong hands, exposing you to theft and fraud.
- File them. Making a digital file of your passwords and leaving it on your devices can be dangerous if someone gains access to your computer, smartphone, or tablet.
- Make it simple. Many people use the same password everywhere, often one that is easily guessed (e.g., 123456, a birthday, home address, pet name, spouse name, child name). But if hackers crack it once, they can use it to access all your sites.
- Let your browser do it. Most browsers can remember passwords. But if not managed correctly, the browser might automatically log you in and expose your accounts to anyone who uses your device, or make your saved passwords accessible to outsiders.

A new class of tools to minimize the hassle is provided in all recent antivirus tools in which number of password management products have been developed that simply save and auto fill information which make it easy to call up passwords and access them securely and conveniently whenever and wherever needed across all your devices. (Norton By Symantic)

2.5.3 What's a VPN? Your key to online privacy

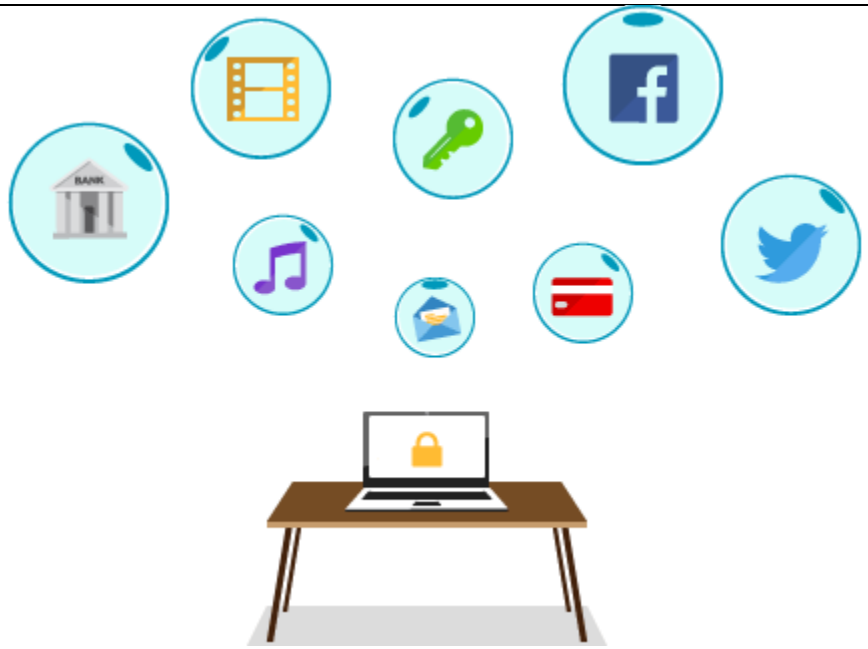


Figure 2.4 : VPN (Virtual private network)

A VPN (virtual private network) is a service that encrypts your Internet connection and hides your location to give you total online privacy.

Table 2.5 : Top 3 reasons to use VPN

1		**Encrypt what you do online** Bank-grade encryption helps stop others from spying on you.
2		**Secure your Wi-Fi** Safely go online at any coffee shop, airport, or park
3		**Visit websites in other locations** Disguise your location to access sites around the world.

(What is VPN?Your key to online privacy)

2.5.4 How Much Should You Reveal on Social Media?

Usually we all love sharing stuff on social media like facebook, instagram and twitter. But we should know how much should be shared and what shouldn't be. (slideshare)

Never make following personal information public such as

- Home address
- Phone number
- Date of birth
- Vacation plans
- Photos of loved ones
- Information about your kids
- Grudges about your work
- Any financial information

After sharing such a kind of information you may have to face consequences as

- You could be exposing yourself to predators
- You may become victim of identity theft
- Home burglary while you are out
- Risk of being cyber bulled
- You may fall to prey to social engineering schemes
- It may damage your reputation

To avoid such risk and to remain safe the use of antivirus tool along with tightened facebook security setting is recommended.

2.6 Annual summary reports of Antivirus tools comparisons by various organizations

2.6.1 Av-comparatives summary report 2016

At the end of every year AV-Comparatives releases summary report that collates the results of various tests performed over the year and give the awards and comments on product abilities.

The Product of the Year award goes to the vendor whose software performed best overall in the main test series. Finally, a number of products which reached a very high overall standard are given the Top Rated award. The Summary Reports also include individual reviews of each of the programs tested by AV-Comparatives in the main test series. The reviews cover the program's user interface and everyday tasks such as updating and scanning, to give readers an idea of what the software is like to use in real life, and how well-suited it is to both expert and non-expert users.

Total products of 19 vendors are tested rigorously for windows platform for the ability to protect against real world internet threats without slowing down the PC and to remove malware that had already infected PC. (Antivirus Comparative)

2.6.1.1 Results and Awards

Whilst all of the programs in our test reached an acceptable level overall, some programs outperformed others. In order to recognize those products that achieve outstanding scores in our tests, we have given a number of end-of-year awards that highlight the best results in each test and overall. The Product of the Year, Outstanding Product and Top Rated awards are based on overall performance in the Public Main Test Series; there are also Gold, Silver and Bronze awards for each individual test type. The 2016 Product of the Year Award goes to Avira; Outstanding Product Awards go to (alphabetically) Bitdefender and Kaspersky Lab; Top Rated Products are (alphabetically) Emsisoft, ESET, Tencent and ThreatTrack VIPRE.

2.6.1.2 Overview of tested products

Here we provide a summary for each of the programs tested, with a note of each one's successes during the year. Although the user interface does not affect any awards, we have noted some of the best UI features as well.

Avast won three Advanced+ awards in this year's tests. It took joint *Silver* in the Performance Test.The program is quick and easy to install, and simple to use.

AVG received 4 Advanced+ awards in this year's tests. It wins the joint *Gold Award* for Malware Removal, and joint *Bronze Award* for the Real-World Protection Test. We liked its clear and persistent malware alerts.

Avira is **Product of the Year** this year, receiving Advanced+ awards in all 7 tests. It wins joint *Gold Awards* for the File Detection and Performance Tests, Silver for the Malware Removal Test, and joint *Silver* for the Real-World Protection Test. The menu panel on the left-hand side of the window provides easy access to all the program's features.

Bitdefender is an **Outstanding Product** this year, with joint highest scores overall. It wins the *Gold Award* for the Real-World Protection Test, joint *Silver* for Performance, File Detection and False Positives,and the *Bronze Award* for Malware Removal. The very modern interface design is consistent

BullGuard received three Advanced+ awards in 2016's tests. It took the joint *Silver Award* for False Positives and File Detection. Malware alerts are informative and persistent, and the tiled interface provides easy access to individual components.

Emsisoft is a **Top Rated Product** this year, with four Advanced+ awards. It wins a joint *Silver Award* for File Detection, and joint *Bronze* for Performance. We liked its informative setup wizard, and the very clean and modern inerface design.

eScan received an Advanced+ award in three tests this year. It wins joint *Silver Awards* for File Detection and False Positives. Its tiled interface provides easy access to individual components, and status information about each one.

ESET received four Advanced+ awards this year, and is once again a **Top Rated Product**. It wins joint *Gold Awards* for False Positives and Performance. The program interface is very clean and easily accessible, and help facilities are excellent with that found in mobile devices.

2.6.1.3 Advice on choosing Computer Security Software

There is no such thing as the perfect security program, or the best one for all needs and every user. Being recognized as “Product of the Year” does not mean that a program is the “best” in all cases and for everyone: it only means that its overall performance in our tests throughout the year was consistent and unbeaten.

Before selecting a security product, please visit the vendor’s website and evaluate their software by downloading a trial version. Our awards are based on test results only and do not consider other factors, as there are some important factors (such as available interface languages, price, and support options), which you should evaluate for yourself.

2.6.2 Av-Test News Issue Feb 2017

Over 90 percent of all malware targets Windows PCs. Every second four new samples accure. A lot of work for an antivirus software. But which is the best for Windows 8.1? This test shows. According to the report analysis Bitdefender Internet security, kaspersky internet security and Trend Micro Internet Security are on the top for the protection, performance and usability.

Cyber criminals think like business people, and they have to. Because in their line of business, competition is growing tougher all the time. Finally the efforts they expend – from malware programming, through distribution, right down to monetization – have to pay off financially.

And even if they manage to flout all other laws, they are forced to conform to those of the marketplace if they want to be successful. This is also confirmed by the numbers in this year‘s security report from AV-TEST.

The number of malware has grown steadily since the initial tests by AV-TEST in the year 1984. Upon completion of this report, the number of known malware for Windows PCs in the AV-TEST database was at 578,702,687, with strong signs of growth. Currently, 12 million new Windows malware samples come "onto the market" each month. And so it is safe to assume that the number of malware programs targeting the Redmond operating system will break the sound barrier of 600 million even before the end of this year. (av-test.org, 2016)

2.7 Gap Analysis

- Majority of publications giving insight of types of viruses, life cycle of virus, history, major attacks, prediction about future types of malwares
- Many authors have described antivirus tools, types of antivirus, working of antivirus, advantages and limitations of antivirus tools
- Some papers have analysed performance of selected security tools
- Limited research work on management of antivirus tool for personal computer is noticed
- Security awareness for computer literate is present but it is missing for layman computer user in literature
- Literature is not available regarding performance measurement of antivirus tools for personal computer users in Pune region
- Usually most of the users are using antivirus tool as safeguard but they are not utilizing it effectively and efficiently
- Service provided by the antivirus company to the personal computer user needs to be studied and measured
- Personal computer user purchases the antivirus tool. But on what basis user selects the antivirus tool whether cost or performance or service is to be investigated.

2.8 Conceptual background of virus

2.8.1 Virus

VIRUS stands for-Vital Information Resources under Siege. As characterized A computer virus is a self-imitating program containing code that unequivocally duplicates itself and that can ‘infect’ other pro-grams by modifying them or their environment such that a call to an infected program implies a call to a possibly evolved copy of the virus. It is a set of guidelines that control the functions of your computer's operating system. 'Virus' is actually a generic term for software that is unsafe to your system. They spread via disks, or via a network, or via services such as email. Irrespective of how the virus travels, its motivation is to use or damage the resources of your computer. The first viruses were spread as part of computer pro-grams, or by hiding in floppy disks. Most

modern viruses are distributed by Internet services, in particular email. Malicious software or malware for short, are “programs deliberately intended to perform some unauthorized - often harmful or undesirable act." Malware is a generic term and is used to describe many types of malicious software, such as viruses and worms. (Mok, 2004)

A typical structure of a computer virus contains three subroutines. The first subroutine, taint executable, is responsible for finding available executable files and infecting them by copying its code into them. The subroutine do-damage, also known as the payload of the virus, is the code responsible for delivering the malicious part of the virus. The last subroutine, trigger-pulled checks if the covered conditions are met to convey its payload. (Wielputz, 2007)

2.8.2 Working of computer virus

Computer viruses have a life cycle that begins when they're created and ends when they're completely removed. The following diagram depicts each stage in the life cycle of computer virus. (Pele Li, 2008)

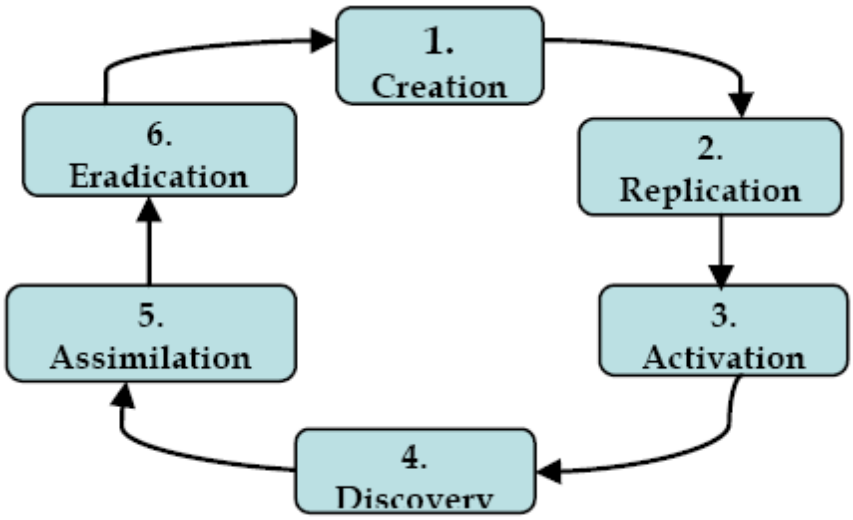


Figure 2.5 Life cycle of Computer Virus

- **Stage I - Creation** – The Computer viruses are created by misinformed individuals who wish to cause widespread, random harm to computers.
- **Stage II -Replication -** Computer Viruses reproduce by nature means it duplicates itself from one PC to anther PC.

- **Stage III –Activation -** Viruses that have damage routines will initiate when certain conditions are met. Viruses without damage routines don't activate, instead causing damage by stealing storage space.
- **Stage IV -Discovery -** This phase doesn't always come after activation, but it normally does. Discovery ordinarily takes place at least a year prior the virus might have become a risk to the computing community.
- **Stages V -Assimilation -** At this point, Anti-virus designers adjust their software so that it can detect the new virus. This can take any-where from one day to six months, contingent on the developer and the virus type.
- **Stage VI -Eradication -** If enough users install up-to-date virus protection software, any virus can be wiped out. Viruses can not disappear completely, but some have long ceased to be a major threat.

2.8.3 Classification of computer virus

Regular expansive number of viruses is created. It is type of vindictive software called as malware. The reason of malware creation is to prevent the smooth utilization of computer.

They are generally divided into number of classes, depending on the way in which it is introduced into the target system and the sort of policy breach which it is intended to cause. As it is difficult to define malware appropriately, it can also be difficult to classify malware into distinct categories. Malware is constantly evolving and is also combining different ideas and techniques. For the purpose of this guide, a *payload* is a aggregate term for the actions that a malware attack per-forms on the computer once it has been infected. Commonly, each virus will just taint one sort of target - however some security experts trust that future viruses will be equipped for affecting more than one kind of target. To get a review over the malware-field a classification of the diverse sorts of malware would be of great help. The malicious code are mainly characterized in to five main category which are namely as virus, worms, Trojan or Trojan horse, Obfuscation Technique based virus. Each main category of malicious code is classified in different sub classifications which are shown in bellow figure. (Bhaskar Patil, 2014)

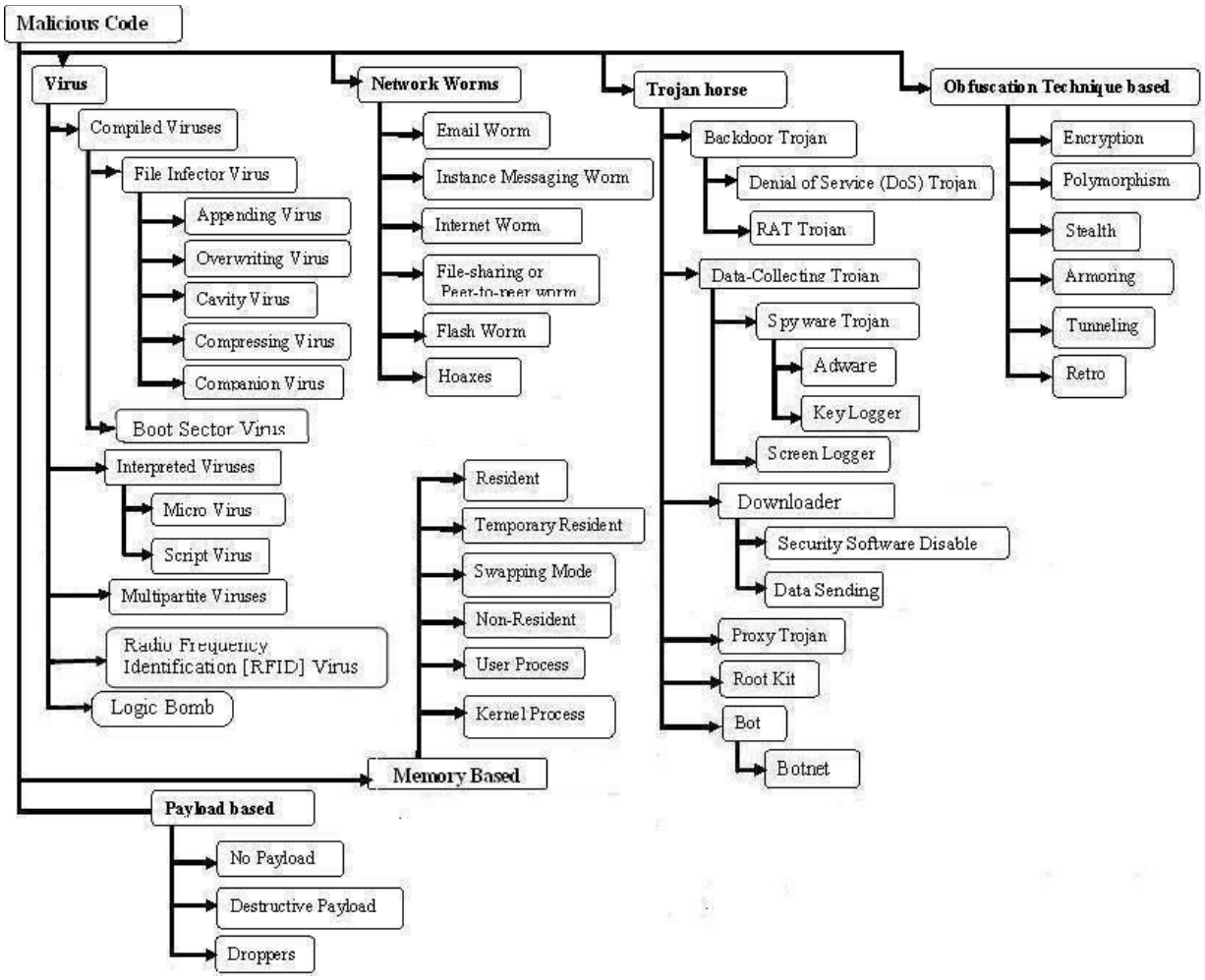


Figure 2.6 Classification of computer virus

2.9 Conceptual background of antivirus tools

2.9.1 Antivirus Tool

"Antivirus" is protective software designed to defend your computer against malicious software. Malicious software or Malware includes: viruses, Trojans, keyloggers, hijackers, dialers, and other code that vandalizes or steals your computer contents. Anyone who does a lot of downloading, or accesses diskettes from the outside worldon a regular basis should develop an antivirus strategy. (Mr. Bhaskar Patil, 2010). Antivirus software is equipped with features that not only check your files in your system, but also check your incoming and out-going e-mail attachments for viruses and other malicious programs.

2.9.1 Types of Antivirus Tool

Antivirus products are categorized into three parts such as Internet Security [IS], Total Security [TS], and Antivirus [AV]. Antivirus: products are the products, which are primarily focused on detecting and remediation viruses and Spyware. Internet Security product provides all the virus and Spyware removal features of an AV, as well as extra functions to provide greater Internet protection. These features may include protection against phishing, root kit detection, firewalls and scanning of web pages and HTTP data. Total Security: products provide data migration and backup features on top of all security features common to IS products (Paul Royal) with mobile security, safe banking and parental control.

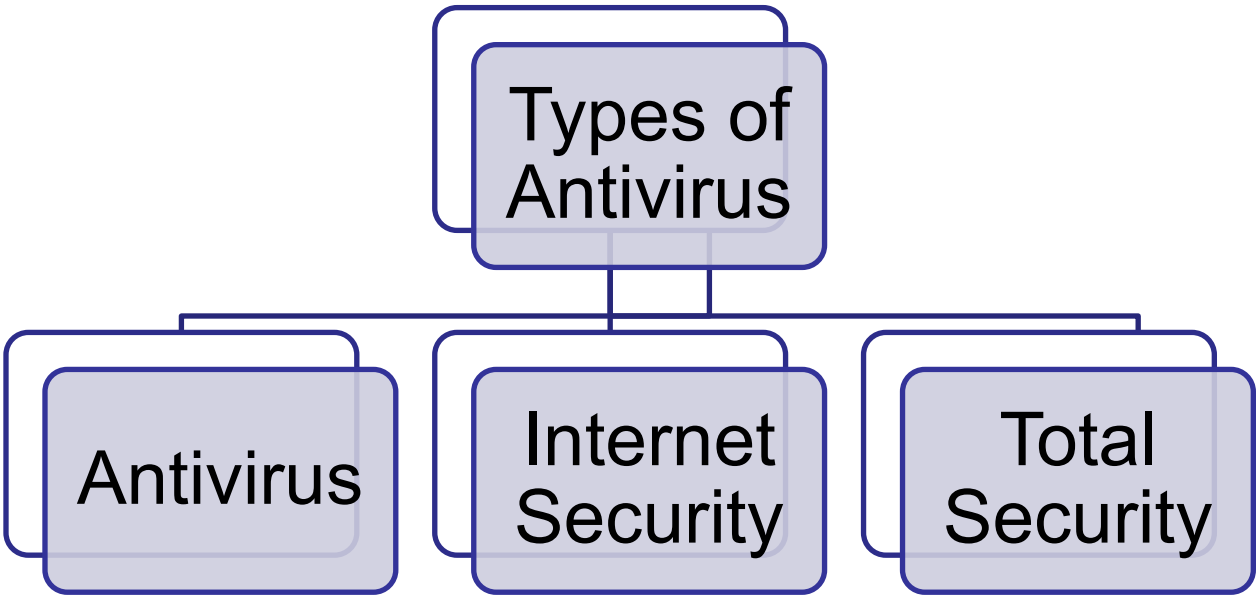


Figure 2.7 Types of Antivirus

2.9.2 Working of Antivirus Tool

The use of computers and Internet are increasing day by day for different purposes with more and more users. In the meantime these computers and networks are confronting number of issues postured by malicious codes like virus, Trojan, worms etc.

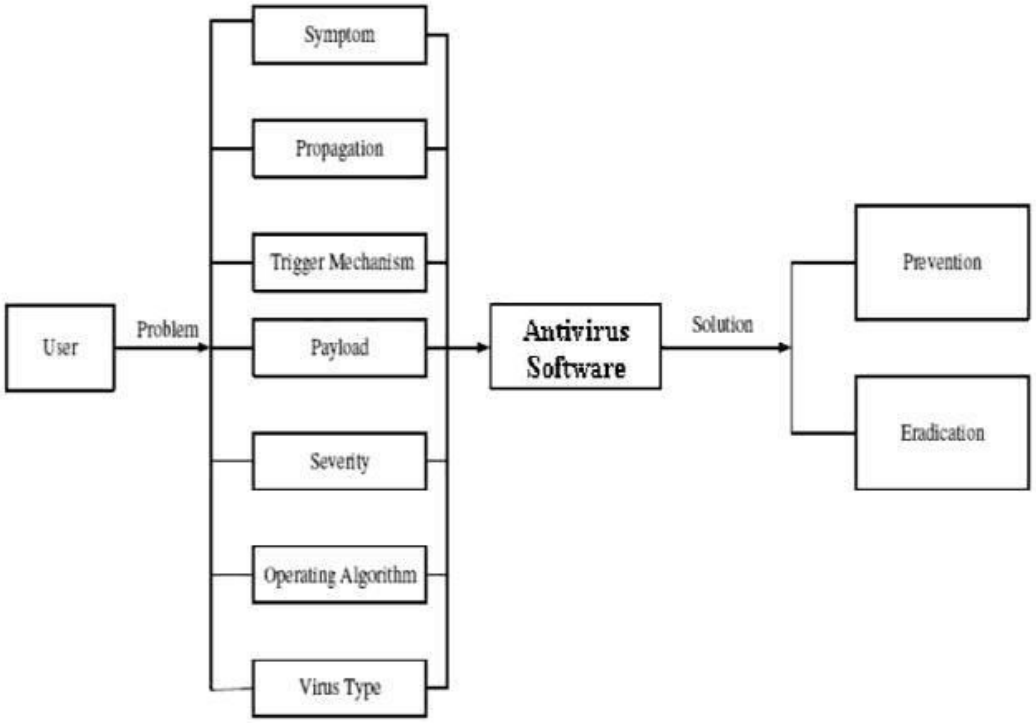


Figure 2.8 Problems faced by Antivirus Tool

The above figure describes the problem such as Symptoms, Propagation, Trigger Mechanism, Payload, Security, and operating algorithm. These different problems are faced and analyzed by Anti-virus software programs, which provide solutions for prevention and eradication of computer viruses and provides the computer user peace of mind and right to stay safe in digital life.

2.9.3 Virus Detection methods

According to Frederick Cohen "No antivirus tool can perfectly detect all possible viruses". However, using innovative method of defense, a better detection rate may be gained. Following figure depicts the different methods which antivirus engine can use to prevent, detect and eliminate malwares.

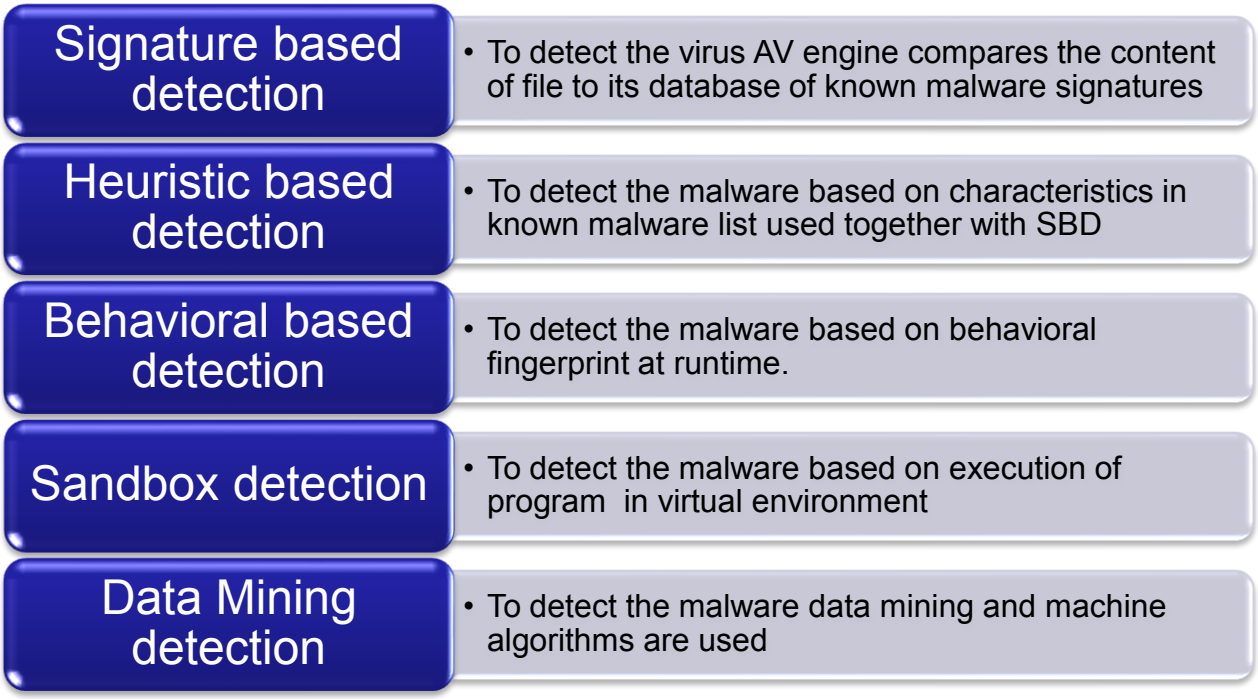


Figure 2.9 Virus detection techniques

2.10 Summary

In the first part of literature review the researcher has studied the research papers, articles, books and thesis related to the computer virus , history of computer virus, it's types, major computer attacks, it's effect on the IT industry, how to mitigate it and how to prevent it. In the second part the antivirus tools, history of antivirus tools, detection methods and types of antivirus tools is elaborated. In most of the papers authors has illustrated the security tips to be followed by internet users to avert and combat with major threat of computer viruses and malwares. Also the listing and details of worldwide organizations providing systematic antivirus testing that checks whether antivirus tools lives up to its promises by creating a real world environments using largest sample collections worldwide. This will guide the computer user for the selection of antivirus tools depending upon the user requirement. Further the detailed study and product wise characteristics of selected companies' security tools are depicted in tabularised format. Also the researcher has provided the brief description of conceptual background of virus and antivirus tools.

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Introduction

Large number of PC users has now become familiarized with the existence of computer viruses and the internet treats. Viruses are a fact of life and the rate at which the new viruses are created is very fast. Also it is continuously increasing due to interconnectivity and interoperability among the world's PC users which are beneficial to users but also the desirable state for fast propagation of computer virus. Hence to safeguard the computer the use of antivirus tool is recommended.

This research aims to study the management of antivirus tool for personal computer security through survey method. Survey conducted for PC users and vendors of antivirus tools in Pune city intended to study the selection, usage and awareness of antivirus tool among the personal computer users.

3.2 Statement of the research problem

Computer security is not like forestry where you plant a sapling and abandon it - it is more like bonsai, where steady nurturing is required. This includes selection, updating and management of antivirus tool data and programs, patching the operating system and applications, and running anti-spyware and firewall programs. (Gregory, 2004)

Hence the Antivirus tool must be used to protect PC. Antivirus Tool is specifically written to defend a system against the threats that malware presents. Antivirus Tool may work differently and ranges from large security packages to small programs designed to handle a specific virus.

The large number of Antivirus Tool available in the market and some are being launched, each one of them offers new features for detecting and eradicating viruses and malware. Consequently individuals have a variety of different types of Anti-virus i.e. both in the

form of freeware software or licensed software available in market. Hence it is really difficult to select the proper antivirus tool. The choice of the perfect antivirus tool depends upon the personal needs and the preferences of particular PC user.

- Some antivirus tools offer fast and efficient execution which is well suited for laptops and older computers.
- Some are easy to manage and can be used by inexperienced computer users.
- Some have additional features like safe online banking and browser sandbox protection which will be useful in these days of digital online transactions.
- Some antivirus tools provide very good protection at reasonable rate.

While selecting antivirus tool every personal computer user has to take a look at honest benchmark and decide how much to spend and what features value the best for them. Hence there is a need to find best Antivirus Tool whose performance is good and also suitable for the specific needs of the users with reasonable price.

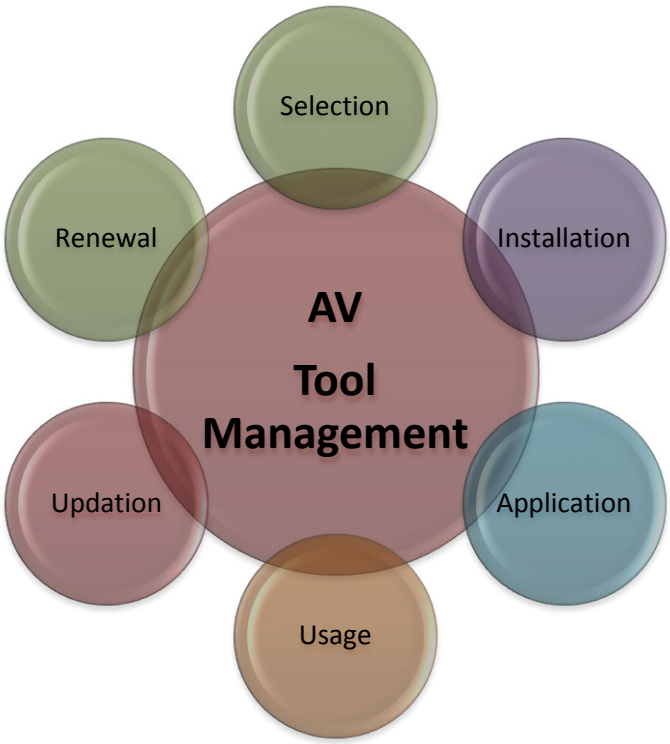
In this contest "How to manage the antivirus tool for personal computer security?" is a question to be tackled. Researcher seeks to study the policies related to selection, installation, application, usage, updating and renewal of AV tool. The study is further indented to find active methods which include avoidance, detection and cure rather than only prevention.

3.3 Rational of the study

Since personal computers playing vital part in vast majority's digital lives today, it has become as important to protect one from computer viruses, malwares and cyber threats, as from real-life flu outbreaks. In spite of the fact that many companies offer free versions of their security software suites, these are frequently significantly stripped down versions of the full-featured package. So as to be completely protected, it is wise to purchase a total security package from a trusted developer. These days it is difficult to choose the right antivirus product because large numbers of products are available in the market. Investing in quality antivirus and security software can be considered as imperative as having insurance, in that it shields the user from having to pay expensive

repair costs later on. Likewise, the more computers around the globe that are fully protected against malicious code the harder it is for viruses to rapidly propagate across the web.

Dealing with cyber threats should not only involve the best damage control approach but proactive management of antivirus tool also. Managing antivirus tool refers to policies related to selection, installation, application, usage, updating and renewal of antivirus tool



for that internet connection is must.

Figure 3.1 Management of Antivirus tool

After all, keeping the milk from spilling over is always better than mopping it.

This research is intended to offer a suggestive action plan for management of antivirus tool so that to attain personal computer security from all the internet treats and malwares.

3.4 Scope of study

The researcher has considered the Pune.(Wikipedia) urban region for the study, since Pune is the second biggest city in the western Indian state of Maharashtra. It is known for its educational facilities, having more than a hundred educational institutes and nine universities, and its growing industrial facilities. Pune is an administrative centre and now vital modern industrial point with reference to IT. Refer Annexure 3

During the course of the present study, the researcher has collected data from the various Banks (Nationalized and International), Insurance companies, Government offices, colleges, private industries, business, housewives etc. For collection of data, various parameters are used like types of antivirus tools, its usage and its impact on various users, security , comparative study of prevention and protection measures of various antivirus tools , threat detection etc. By doing the analysis of primary data, researcher has suggested safety awareness measures for the usage of personal computers for the various types of the users.

The researcher has restricted the investigation to

1. Pune Urban area only
2. Antivirus users of personal computers (Students, Working Professionals & housewives)
3. Antivirus Vendors

3.5 Objectives of the study

Researcher has conducted empirical research work on the basis of set objectives, the objectives are as follows;

- To study the awareness of various antivirus tools for personal computer users
- To study the selection criteria of antivirus tool
- To identify the usage of antivirus tools and its impact on various users
- To do comparative study of prevention and protection measures of various antivirus tools
- To study the reason behind the popularity of antivirus tool

- To study the services provided by Antivirus company
- To study the Services provided by antivirus provider companies support/Help center

3.6. Hypothesis of the study

3.6.1. Hypotheses

In consistence with the objectives, hypotheses have formed by the researcher for study purpose

H_1 : "As a security reason, personal computer users are highly using licensed edition of antivirus tools".

H_2: "Managing antivirus tool is utmost necessary for safe use of personal computer".

H_3: "While purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand"

3.6.2. Description of Hypotheses

H_1: "As a security reason, Users are highly using licensed edition of antivirus tools".

This hypothesis has been tested by using the usage of licensed and free version of antivirus tools used by the user by using percentage and Z-test. For testing the hypothesis, various parameters were also considered like edition version of antivirus tool like Licensed, trial. These parameters are based on the questionnaire of users. (**Annexure 1 and Q.4**).

H_2"Managing antivirus tool is utmost necessary for safe use of personal computer".

This hypothesis has been tested by using Managing antivirus tool is at the most necessary for safe use of personal computer by using percentage and 3 point Likert scale applied for the same. These parameters are based on the questionnaire of users (**Annexure 1 and Q.21**).

H_3 "While Purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand"

This hypothesis has been tested by using , While Purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand and Z – test. For testing the hypothesis, various parameters were also considered like Brand, Service and Price. These parameters are based on the questionnaire of users (**Annexure 1 Q. 12)**.

3.7 Research Methodology

This research study is related to the usage and an impact of antivirus tools used for personal computers in Pune city and suggests a action plan management of antivirus tool to attain personal computer security from internet threats and malware. The secondary data exploit already available information both published as well as unpublished. For primary data, however, such a facility is not available and it has to be collected by the survey method.

The survey is undertaken by the researcher for acquiring a sample by using a **Purposive and Quota** (C.R.Kothari) (Gupta) sampling techniques. Research methodology used for the purpose of obtaining sample and collection of primary data from them along with nature of sample and sample size.

Primary and Secondary data is compulsorily required and essential for analysis of study objectives and to accomplish the goal of the objectives. Primary data is collected through survey method by administering a questionnaire and separate structured interview with higher authorities related to various working professionals, vendors, students and house wives from Pune urban area.

The methodology adopted is a mixture of literature review, document analysis such as interview with higher authorities or officer in the organization, various reports from Antivirus Tool and computer virus testing labs. The researcher has reviewed existing literature on Antivirus Tool performance and different types of current viruses to understand the context and critical issues of the problem. This learning was supplemented with discussions with various users of computers such as students, vendors, businessman‘s, housewives and other users.

3.7.1 Primary Data

Primary data is obtained through a survey and such data is original and first hand in nature. Primary data is collected using various methods like telephone survey/e-mail survey, mail questionnaire, personal observation and interviews. Particularly in survey, the important ones are – observation, interview, questionnaire, schedules, telephone and survey (C.R.Kothari) etc. The primary data collected by the researcher is explained in the following manner:-

A) Selection of the city

The researcher has used purposive sampling method to select the city for the purpose of the study. The researcher has selected Pune City as it is center of IT hub and also "The Oxford of the East". The researcher has also find out that there is scope for the increasing security during online transaction and suggest an action plan for management of antivirus tool for personal computer users in Pune city.

B) Selection of the Respondents

For study purpose two respondents were selected

1. Users of Antivirus Tools
2. Vendors

Table No.3.1: Sample size

Type of Respondents	No. of Respondents	Total Sample Size
Users	384	411
Vendors	37	

B.1) Selection of users

The researcher has used **purposive and quota sampling method** for the selection of various types of users from Pune city. A study is also focused on various types of

antivirus tools and their usage by the users along with maintenance of antivirus tools by their vendors.

As per the 2011 Census of India estimate, the population of the Pune urban agglomeration is 6,226,959. The population of Pune on May 19, 2014 is approximately 8,242,142. (Extrapolated from a population of 3,337,481 on July 31, 2009 and a population of 6,115,431 on September 30, 2012.)

Population : 8,242,142

Out of this 32.4 % of users are using computer/laptop. i.e. 267045

So actual population consider for sample calculation is 2670454

To determine the sample size in the study, Krejcie Morgan's table 1970 (Refer Annexure 5) of determining sample size for known population is used. Accordingly for a population equal to or greater than 1000000 the required sample size is 384. Hence for a population of size 2670454, the sample size is fixed as 384.

Following table shows the Sample size of Antivirus Tool Users in Pune urban area which are well thought-out for this study. Researcher has undertaken the study of users of Antivirus tools, hence only registered users of Antivirus tools are considered for deciding sample. Total 384 users are selected as samples for study purpose.

Personal computer is a small and relatively inexpensive computer designed for use by one user at a time. It can be in the form of desktop, laptop, notebook, palmtop or tablet. Most of the times, the whole family shares the same PC to accomplish different tasks depending upon their needs. Family members are from different ages, positions and computing background providing ideal situation for computer viruses to grow. There is large community of personal computer users in Pune. Every person working in public or private sector is using computer daily to perform their everyday tasks. Also the students are using computer for effective learning, online examinations, browsing, social

networking and playing games. House wives are also using computer to pay bills, social networking and to teach their children basic computer operations. By analyzing the types of personal computer users, it is found that more working professional are using personal computers followed by students and house wives. Hence the researcher has decided following sample size of users depending upon the usage.

Table No.3.2: Sample size of Antivirus Tool Users

Type of Users	No. of Users	Total No. of Users
Working Professionals	222	384
Students	125	
Housewives	37	

B.2) Selection of the Vendors

Table No.3.3: Sample size of Antivirus Tool vendors

Antivirus Companies	Total No. of Vendors
AVG	37
Kaspersky	
McAfee	
Net Protector	
Norton	
Quick Heal	

In order to study the antivirus tools, the researcher has selected 37 vendors from 14 wards of Pune city based on various types of antivirus tools. Actually the data from (14 wards * 3 vendors) = 42 vendors was collected but some vendors didn't answered properly and due to sampling error data from 37 vendors was analyzed. Also the main aim of

researcher is to study the managing of antivirus tool for personal computer users in Pune city, hence the more weightage is given to the data collected from antivirus users questionnaire. The vendor's data is collected to support the study. Also with the personal discussion with antivirus vendors and doing the market survey for most frequently used antivirus tools by Pune citizens, the researcher has fixed the above five companies products for study.

D) Sample Design:

The study aims at collecting data from the various users those who uses Antivirus Tools for their personal computer. From the pilot survey, it clears that most of the users uses antivirus tools for their personal computer to maintain the security of their personal and professional data. Hence researcher concludes that the entire users of personal computers comprise the universe for the study.

3.7.2 Secondary Data:

The secondary data is collected from existing published and unpublished data like various national and international journals, magazines. Conference proceedings, Govt. reports etc. and which will be further used for analysis of objectives and testing of hypotheses wherever required. It is also helpful for the construction of objectives and hypotheses of the present study. Apart from these, other sources of secondary data are as follows:

(i) Annual reports of antivirus labs
(ii) Departmental publications of antivirus labs
(iii) Worldwide computer virus database from internet
(iv) Training Material and manuals are used in various antivirus labs for pertaining to computerized information system.
(v) Libraries in and around Pune city.

3.7.3 Questionnaires:

One questionnaire (C.R Kothari) (Gupta) was prepared for antivirus users. It contains information about antivirus tools, antivirus software and updating period of antivirus. It also relates to importance of antivirus software security, Malware detection, Firewall security, Web page scanning, scanning speed, update frequency, cost and also to discuss with users regarding aspects of technical support in terms of online support, Telephonic support, support through Email, User manual, User Forum. it also study the aspects related to the scanning capability of the present Antivirus Tool in regards of On-access scanning, On-demand Scanning, Scheduled Scanning, Manual Scanning, Compressed File scanning, Auto cleaning infected files, Email-protection, File Sharing protection, Web Mail protection, Heuristic Scanning, Ad ware / Spyware Scanning, Script Blocking etc.

Second set of questionnaire is for Antivirus vendors in Pune city. It focuses mainly on Antivirus tools which are supporting for single or multiple devices. The research has collected data from vendors in Pune city. The researcher has applied the following measurement framework for identifying key areas of direct and indirect qualitative and quantitative data about usages of antivirus tools.

In these questionnaires, researcher has focused on following key areas-

a. Popular Antivirus software
b. Total cost of Antivirus software for single/multiple users
c. Cost of Internet security software for single/multiple users
d. various services providing while purchasing the antivirus
e. Popularity of antivirus

3.7.4 Contact method:

The respondents have been contacted personally for getting the questionnaire filled up along with google docs. This has ensured obtaining more accurate and relevant information from the respondents. Also Personal Interview with structured questionnaire has been conducted with various antivirus tool vendors. It has been conducted to

understand the problems of users while using personal computer regarding selection, installation, usage, applications and updation, renewal of antivirus tools.

3.8 Limitations of the study

Even though all attempts are made by the researcher to make a comprehensive study of usage and impact of antivirus tools on personal computer users, there are limitations observed by the researcher, which are as follows. The work was started by visiting the owner, manager and end user of different organizations. In first few visits, general information was collected. The researcher has observed following limitations during research work.

1. It was very difficult situation to get an appointment of the officers and convey them to the importance of the research work.
2. The most of professionals working in organization like banks, hospitals, owners were not interested to accept the questionnaire and discuss the issues due to work load.
3. Some respondents were hesitating to provide information due to secrecy of data and records.
4. Some respondents frequently change their Anti-virus software. Thus they not familiar with questions which are asked in questionnaire.
5. Only the windows operating system is considered for study. Other operating systems like MAC, Linux are not considered.
6. Antivirus tools for mobiles are not taken for study due to the limitations.

3.9 Period Covered In Years:

Researcher has covered time period for the research work from 2011 to 2016-17 to consider the major practices in the area of Antivirus Tools used by users for their personal computers and vendors.

CHAPTER 4
DATA ANALYSIS
AND INTERPRETATION

4.1 Introduction

The study is related to the management of antivirus tools for personal computers in Pune city. The researcher has used survey based research methodology to carry out this research. This research is related to the antivirus tool management for personal computers with special reference in Pune city. The researcher has tested positively the hypotheses of this research study, with the help of primary and secondary data. For the purpose of the study, samples are divided into two parts. Part I is about users of antivirus tools comprising of working professionals, Students & Housewives who uses various services of antivirus tools and Part II is about Vendors of antivirus tools.

The researcher has selected two types of samples and collected data from them. The first sample consists of 384 Antivirus tools users . The second sample has 37 vendors of Pune city from 4 zones including 14 ward offices

. They are shown in Table No.4.1

Table No. 4.1: Selection of Sample

Sample No.	Constituents	Number of Sample points in the sample
1	Antivirus Tools Users	384
2	Vendors	37

The data is collected through interviews and questionnaires and compiled in 30 tables for Users, 7 tables for vendors and further 2 for hypotheses testing. Statistical parameters and graphics have been used wherever necessary and useful. The data analysis is grouped in 2 parts as follows:-

Presentation and Analysis of Data I: Users of Antivirus Tools

In Part I, the primary data about 384 users from 14 ward offices of Pune city has been collected by the researcher (Para 3.7.1 B1). An analysis is carried out under four broad headings as follows:

1. Background of Respondents according to their Education and Computer Technology Background**.**
2. Awareness of various antivirus tools for personal computers.
3. Usage of antivirus tools and its impact on various users
4. Comparative study of prevention and protection measures of various antivirus tools

Presentation and Analysis of Data II: Vendors

In Part II, the primary data has been collected by the researcher with respect to 37 vendors from Pune (Para 3.7.1 B2). For the purpose of the study, the researcher has selected vendors from 14 ward offices of Pune city. The vendor analysis is carried out under Two broad headings and is as follows:

1. Services provided by antivirus provider companies and its impact on various users.
2. Impact of Cost while purchasing Antivirus tools

4.2 Pilot Survey

The researcher has conducted pilot survey randomly to test the questionnaire. To know the consistency of questionnaire to be administered for the research, researcher has applied the Cronbach's Alpha reliability test. Initially the questionnaire was circulated to 12 Vendors & 56 users and reliability test was conducted.

The result of pilot survey about vendors is given in following Table No. 4.2 and about users in Table No. 4.3 respectively.

Table No. 4.2: Reliability Statistics of pilot survey of Vendors

		No. of Respondents	%	Cronbach's Alpha	N of Items
Cases	Valid	12	100.0	0.947	147
	Excluded[a]	0	0.0		
	Total	12	100.0		

a. Listwise deletion based on all variables in the procedure

It is observed that questionnaire is consistence and Cronbach's Alpha score is 0.947. It means 94 percent respondents understood the questionnaire. Thus researcher concludes that this questionnaire can be administered for the further research.

Table No. 4.3: Reliability Statistics of pilot survey of users of Antivirus tools

		No. of Respondents	%	Cronbach's Alpha	N of Items
Cases	Valid	56	100.0	0.925	97
	Excluded[a]	0	0.0		
	Total	56	100.0		

a. Listwise deletion based on all variables in the procedure

It is observed that questionnaire is consistence and Cronbach's Alpha score is 0.925. It means 92 percent respondents understood the questionnaire. Thus researcher concludes that this questionnaire can be administered for the further research.

4.3 Issues related to users of Antivirus Tools

In today's IT world, technology is moving very fast. We spend most of our time on internet which is an integral part of our life. Our activities include socializing with friends on social media network, work online and shop online. For all purposes including regular need, office work etc, and user wants online services for saving their time as well as efforts. But this information highway is puzzled with malware threats and due to the worldwide connectivity it spreads very fast. So everybody wants the secure internet access and safe personal computers use for performing computing activities. Because Common user community of computer can suffer from some sort of exponentially increasingly problem of computer viruses due to inadequate protection mechanisms and infrastructure initiatives. So need to study about various Antivirus tools available in the market and find out the best one.

4.4 Background of Respondents according to their Gender, Education and Computer Technology knowledge

Pune, the Oxford of the East and hub of Information Technology is also a historical city in India with a glorious past, an innovative present and a promising future. For administrative purposes Pune city is divided into four zones with 14 ward offices.

As a major venue of public access to Information and Communication Technologies (ICT), cyber cafes in India have been contributing to the increase of ICT penetration, especially Internet penetration for the last decades. Although Internet is a vital source of information, it is misused by cyber crooks. These threats range from intellectual property theft, zero-day security vulnerability, spear-phishing to complex attacks. So top antivirus tool is essential which plays the role of AntiVirus, AntiSpyware, AntiMalware, AntiSpam, AntiPhishing, Parental Control, PC2 Mobile, PCTuner, etc. Such AntiVirus software gives multi-layered protection for user PC along with added security for your mobile phones. Only purchasing of antivirus tool and installation of it on personal computer is not sufficient for safe use of personal computer but personal computer users have to tighten security settings of their Antivirus tools to prevent threats and control it as well as avoid them.

To know about the user and their awareness as per their category, need to study their general background which covers their education and computer security knowledge. Such background is essential to ascertain their knowledge about computer literacy, internet literacy and awareness of the computer security management system.

4.4.1 Background of users according to their Gender

In today's IT world users should be educated and should have an adequate knowledge of computers, internet literate as well as cyber security. A combination of good antivirus tool, a little bit of playing around with existing preventive ways and not to forget, increasing the knowledge about internet threats, goes a long way to secure personal computer and reputation of user. To use a computer the person should have a good educational background. Computer Literacy and cyber security is one of the key socio-economic progress measures of modern society and an important aspect of Indian society. According to the latest Indian Population Census 2011, the average literacy rate of Pune city is 91.61 percent and it is high as compared to state and national level average literacy rate.

Table No. 4.4 shows the distribution of users according to their gender. It is observed that there is 50:50 proportion of male: female population meaning that 50 percent citizens are male and 50 percent citizens are female in the sample. When we compare the respondent's population ratio with Pune's male and female ratio, it is at around equal level.

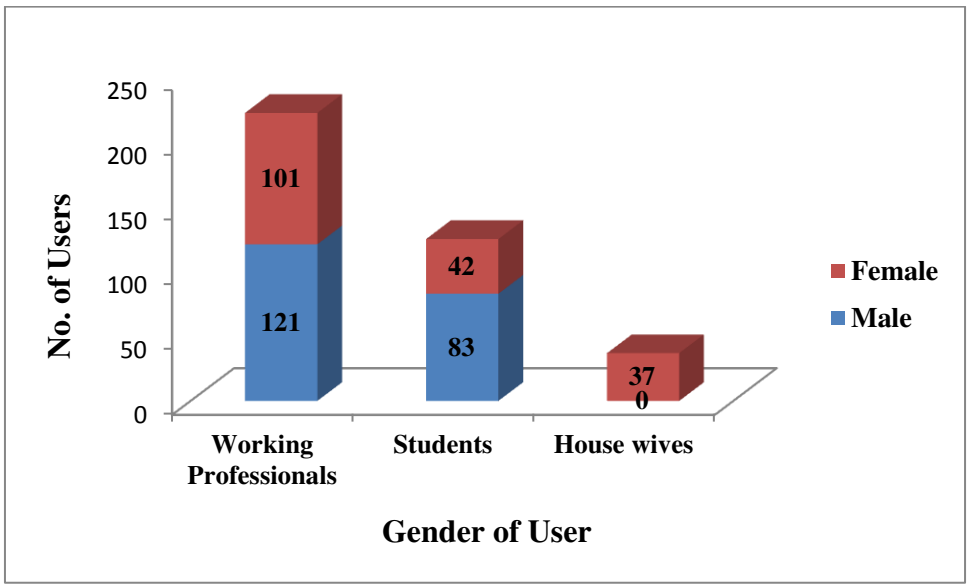
It is seen that 31.51 percent working professionals are male as compared to the 26.30 percent are female respondents. So ratio of male working professionals is higher than that of female working professionals. Whereas 21.61 percent are male students and 10.94 percent are female students. So in student's category, ratio of male students is higher than that of female students. And 9.63 percent house wives contributed and their ratio is very low as compared to other user types.

Table No.4.4: Distribution of Users according to Gender

Gender	Working Professionals	Students	House wives	Total
Male	121(31.51)	83(21.61)	-	204(53.12)
Female	101(26.30)	42(10.94)	37(09.63)	180(46.88)
Total	222(57.81)	125(32.55)	37(09.63)	384(100.00)

Figures in bracket indicates Percentage

Graph 4.1: Distribution of Users according to their Gender



The Graph 4.1 visually displays distribution of users according to their gender. It is clear that majority of the users that is 53.12 percent are male users whereas 46.88 percent are female users. It is clear that ratio of male users is slightly higher than female users. Means in the era of Information Technology, still most of the internet users are male as compared to the female users and they dominate females in this sector.

4.4.2 Background of users according to their Education

Table No. 4.5 represents the distribution of users according to their type and education. It is seen that a majority of over 50.52 percent users are Post graduates. Out of which 25 percent are working professionals whereas 23.18 percent are students and only 2.34 percent are housewives. When we compare the user wise education ratio, most of the working Professionals are post graduates as compared to students and housewives.

It is followed by 33.85 percent users who have completed their graduation & above degree, out of which 24.74 percent are working professionals, 7.03 percent are students and 2.08 percent are housewives.

A further 10.68 percent user has completed their higher secondary education, out of which 5.21 percent are working professionals, 2.34 percent are students and 3.3 percent are housewives. The rest of the 5.47 percent users have completed their education up to higher secondary, out of which 2.86 percent are working professionals and 3.13 percent are housewives.

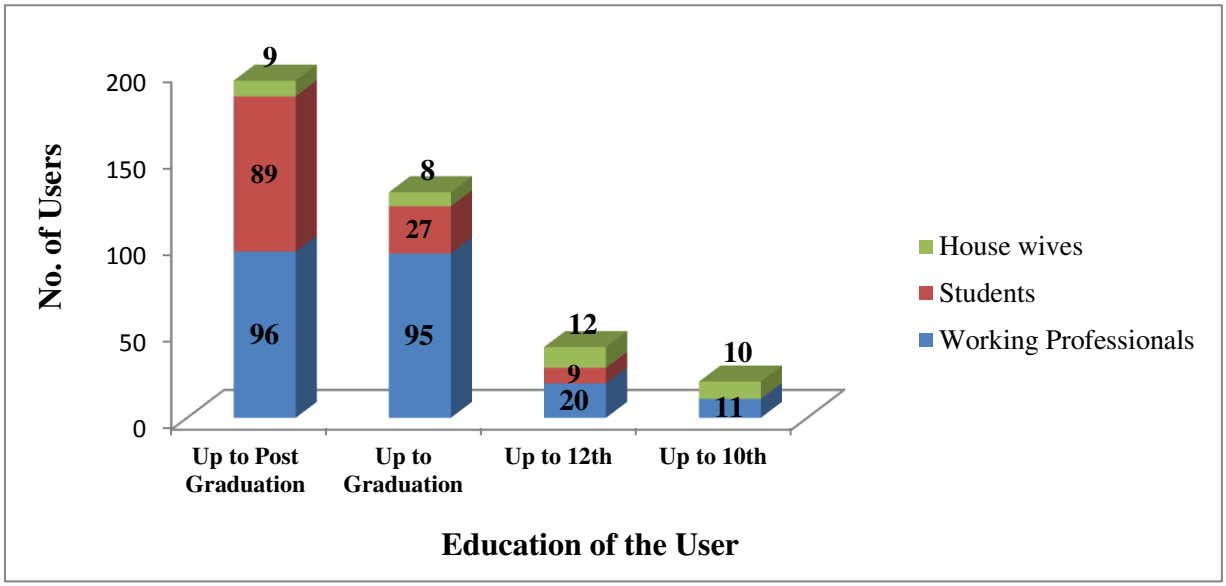
The proportion of Post graduate users is higher to graduate & above user and the proportion of higher secondary & above educated user is higher than higher secondary educated users.

Table No.4.5: Distribution of Users according to education

Education	Working Professionals	Students	House wives	No. of Respondents
Up to Post Graduation	96(25.00)	89(23.18)	9(02.34)	194(50.52)
Up to Graduation	95(24.74)	27(07.03)	8(02.08)	130(33.85)
Up to 12^{th}	20(05.21)	9(02.34)	12(03.3)	41(10.68)
Up to 10^{th}	11(02.86)	0(00.00)	10(03.13)	21(05.47)
Total	222(57.81)	125(32.55)	37(9.64)	384(100.00)

Figures in bracket indicates Percentages

Graph 4.2: Distribution of Users according to their



As can be seen in Graph 4.2, it is apparent that most of the users are Post graduates followed by Graduates, higher secondary and up to State secondary education. While comparing between types of users, it is apparent that , house wives are less educated and working professionals and students are highly educated.

4.4.4 Summary

The majority of the users are male Post graduates and all of these belong to the Working professionals category. It is seen that the response from male user is very high as compared to that of female users in this category of education. The response from post graduate males is also satisfactory as compared to the upto higher secondary education and higher secondary and above education.

4.5 Awareness of Antivirus tools for personal computer

An attempt was made to meet the first objective of the study which is **"To study the awareness of various antivirus tools for personal computers".** The primary data collected from the users has fulfilled this objective. Such an analysis also aims to know the awareness of management of antivirus tools for personal computer in Pune City.

4.5.1 Internet Users

The internet is expanding at a rapid pace and it has already been a player in the field of government offices, business, economy, entertainment and social groups all over the globe. The internet is changing the world and it will continue to do so. The number of internet users is increasing day by day. It has reached 2095 million at the end of 2011, compared to 1,996 million users in the year 2010. The statistics reveal that China has the largest number of users with 513 million and the US is second overall with 245 million. The strongest growth is seen in India which is ranked third where the number of users is 121 million. India – with a billion people still has a chance to get into first position to catch up with the global pace. An analysis of the usage of the internet in the top metro cities in India is given in Table No.1.

4.5.2 Types of user

To study the awareness of Antivirus tools for personal computer, there types of users were considered like working professionals, Students and House wives. To study the awareness of user, parameters such as their education and occupation were considered. Computer literacy and interest in the internet was also considered. If user have an adequate knowledge of computers and are aware about the internet and their threats they can easily use tighten the settings of antivirus tools.

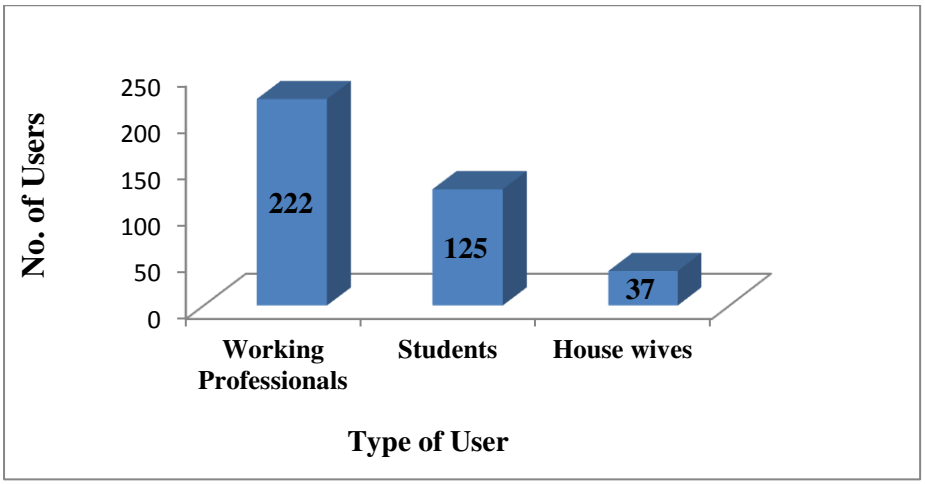
Following Table No.4.6 shows the distribution of users according to their type like working professionals, Students and House wives. It has been observed that most of the working professionals like 57.80 percent are contributed for study followed by 32.60 percent students and remaining 9.60 percent House wives. So ratio of working professionals is higher than that of students and house wives.

Table No.4.6: Distribution of Users according to their type

Type of User	No. of Users
Working Professionals	222(57.80)
Students	125(32.60)
House wives	37(09.60)
Total	384(100.00)

Figures in bracket indicates Percentages

Graph 4.3: Distribution of Users according to their type



Graph 4.3 shows the distribution of user's according to their type like working professionals, students and housewives. As per the above graph total 57.80 percent working professionals contributed followed by 32.60 percent students and 9.60 percent housewives. So ratio of working professionals is high as compared to the Students and Housewives.

4.5.2 Awareness of Antivirus tools among the users

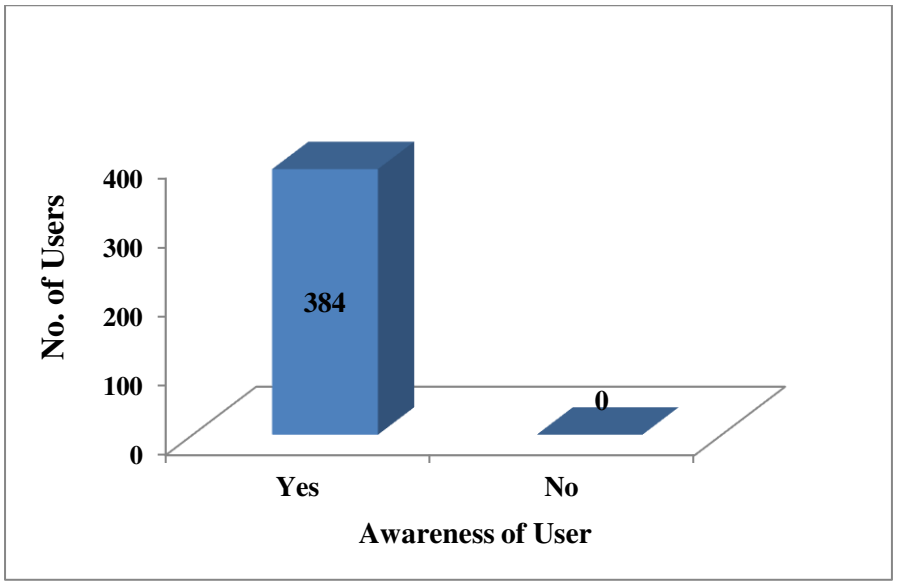
Antivirus tool is one of the most important tools in protecting your computer and personal information from viruses and worms. Without antivirus protection, your computer may be left completely defenseless against perpetrators' relentless attempts. Due to this reason there is need to study the awareness of various antivirus tools for personal computers among the users and which satisfies first objective of the study. Awareness of antivirus tools helps user to keep their personal computers protected from malwares. Following Table No.4.7 shows the awareness of Antivirus tools among the users. From table, it clears that 100 percents users are aware about Antivirus tools.

Table No.4.7: Awareness of Users

Awareness of Antivirus tools	No. of Users
Yes	384 (100.00)
No	0(00.00)
Total	384(100.00)

Figures in bracket indicates Percentages

Graph 4.4: Awareness of Users



Graph 4.4 shows the awareness of antivirus tools among the users. It shows that all of the computer users are aware about antivirus tools so indirectly we can say that they are aware about security of personal information and personal data also.

4.5.2 User wise Awareness

As per Table No. 4.8, all of the users are aware about antivirus tools. As we taken three types of user for study purpose like working professionals, students and housewives, need to identify awareness of antivirus tools among them.

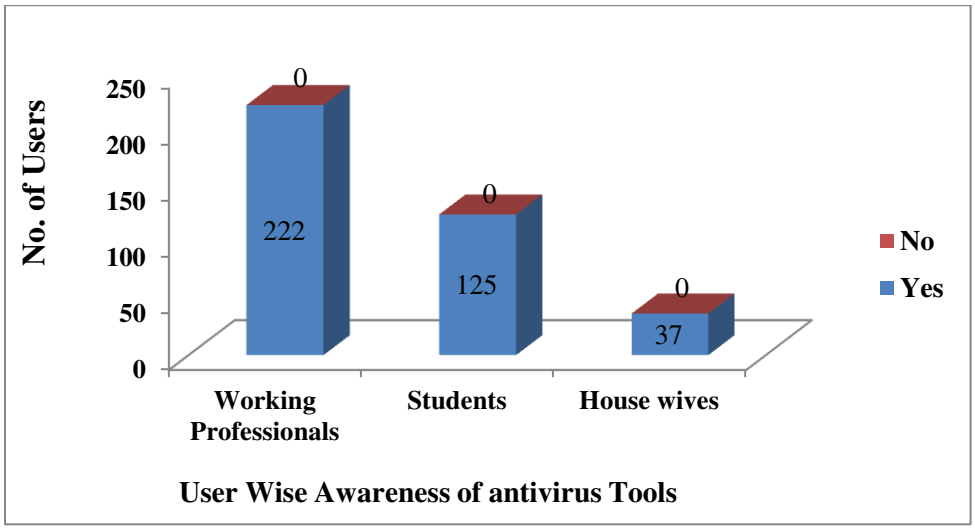
Following Table No. 4.8 shows the use wise awareness of antivirus tools among the user, It is clear that, 57.81 percent working professionals are aware about antivirus tools followed by 32.55 percents students are aware about antivirus tools and 9.64 percents housewives aware about antivirus tools.

Table No.4.8: User wise Awareness of Antivirus Tools

Type of User	No. of Users
Working Professionals	222 (57.81)
Students	125(32.55)
House wives	37(09.64)
Total	384(100.00)

Figures in bracket indicates Percentages

Graph 4.4: User wise Awareness of Antivirus Tools



Graph 4.4 shows the user wise awareness of antivirus tools. It is clear that ratio of awareness of antivirus tools for their personal computers among the working professionals is very high as compared to the students followed by housewives.

4.5.5 Selection Criteria for Purchase of Antivirus Tools

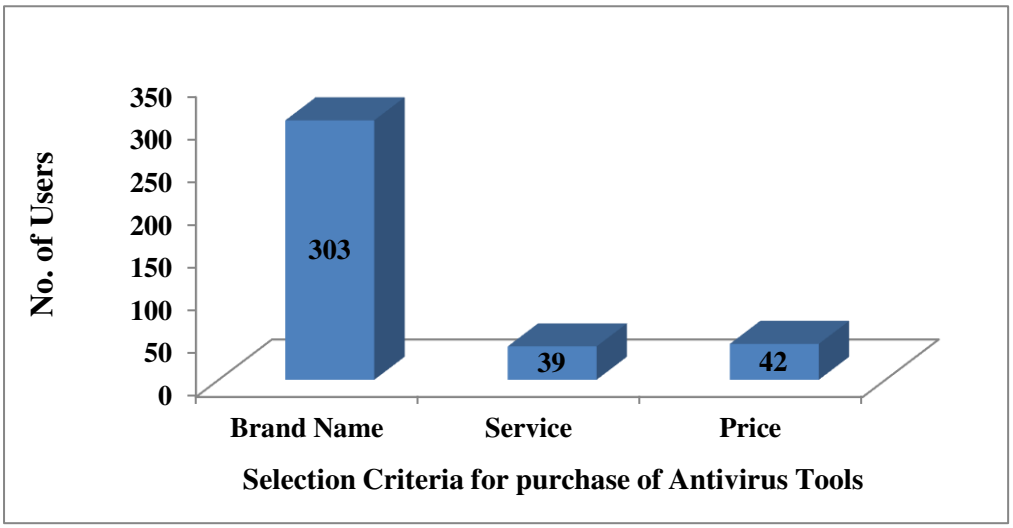
As a need of study, an attempt was made to meet the second objective of study which is " To study the selection criteria purchasing the antivirus tool". It necessary to collect primary data from users regarding selection criteria for purchase of antivirus tool. We have considered Brand name, Service and Price. Table No. 4.9 shows the selection criteria for purchase of antivirus tool. As per the table, it clears that 78.90 percent users prefers brand while purchasing antivirus tool followed by 10.90 percent users prefers price and further 10.20 percent users prefers service provided by the vendor

able No.4.9: Selection Criteria for Purchase of Antivirus Tools

Selection criteria of Antivirus Tools	No. of Users
Brand Name	303(78.90)
Service	39(10.20)
Price	42(10.90)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.5: Selection Criteria for Purchase of Antivirus Tools



Graph 4.5 shows the selection criteria for purchase of antivirus tool. It is seen that most of the users prefers brand while purchasing antivirus tool followed by price and service. So we can say that brand of antivirus tool has a very much positive impact on user.

4.5.6 Summary

The majority of the users are aware about antivirus tools for their personal computer. It is seen that working professionals are highly aware about antivirus tools as compared to the students and housewives to keep their personal computer virus free. It is also seen that while selecting antivirus tools for their personal computer users have high impact of brand of antivirus tools.

4.6 Usage of Antivirus Tools

An attempt was made to meet the Third objective of the study which is **"To identify the usage of antivirus tools and its impact on various users".** The primary data collected from the users has fulfilled this objective. Such an analysis also aims to know the usage of antivirus tools among the various types of the user and effective management of antivirus tools for personal computer.

Originally, Antivirus tools are developed and used to detect and remove computer viruses. Antivirus software runs in the background on your computer, checking every

file you open. This is generally known as on-access scanning, background scanning, resident scanning, real-time protection, or something else, depending on your antivirus program. That's why it is an essential part of a multi-layered security strategy – even if you're a smart computer user, the constant stream of vulnerabilities for browsers, plug-ins, and the Windows operating system itself make antivirus protection important.

4.6.1 Editions of Antivirus Tools

Most of the antivirus Tools are available in Trial/free and Licensed and in both like Trial/free & licensed editions. Trial editions raise awareness of security among the users and once user understands importance, effectiveness & efficiency of Antivirus tools, they automatically purchased licensed version.

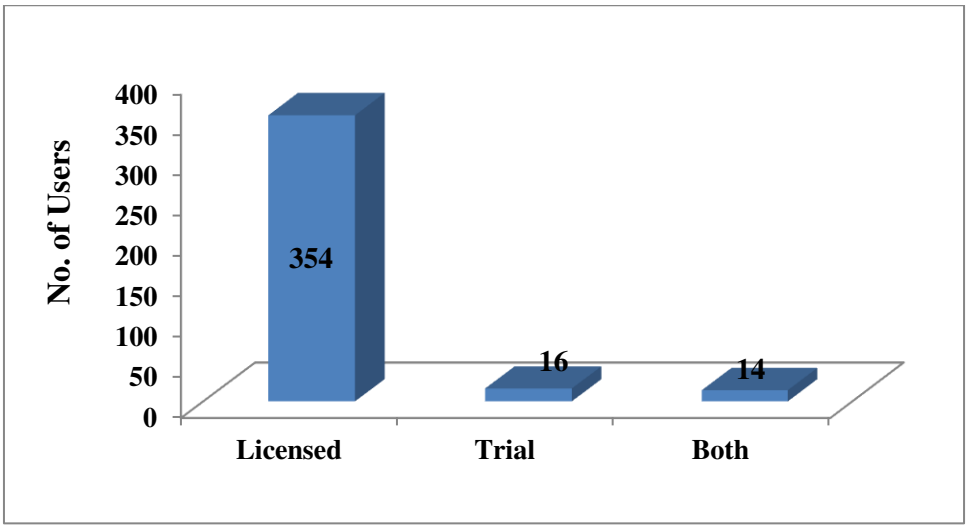
As a part of study, need to identify usage of edition of antivirus tools. It includes three types like licensed, triall or free and usage of both. Following Table No.4.10 shows the Editions of Antivirus trials tools used by the users. It clears that, 92.20 percent user used licensed edition followed by 4.20 percent user used trial edition and 3.60 percent user used both versions.

Table No.4.10: Edition of Antivirus Tools

Version of antivirus tools	No. of Users
Licensed	354(92.20)
Trial	16(04.20)
Both	14(03.60)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.6: Edition of Antivirus Tools



Graph 4.6 shows the edition of antivirus tools used by the user. It shows that most of the user used licensed edition of antivirus tools as compared to the free/trial edition of the antivirus tools. It clears that users are ready to pay for securing their data and personal details and indirectly aware about importance of antivirus tools. It is followed by usage of trial/free edition of antivirus tools and very few users use both editions.

4.6.2 User Wise Usage of Edition of Antivirus tools

As we have considered three types of user for study purpose, so need to identify user wise usage of edition of antivirus tools. There are three types of user like working professionals, students and house wives and three editions of antivirus tools like licensed, free/trial and both. Following Table No. 4.11 shows user wise usage of edition of antivirus tools. It is seen that maximum number of users that is 92.19 percent users licensed edition of antivirus tools. Out of which 55.99 percents are working professionals followed by 26.82 percent are students and only 9.38 percent house wives used licensed edition of antivirus tools.

Whereas 4.16 users use trial edition of antivirus tools out of which only 0.78 percent are working professionals and 2.60 percent are students and only 0.78 percent are house wives. Also it is seen that only 3.65 percent users uses both the editions. Out of

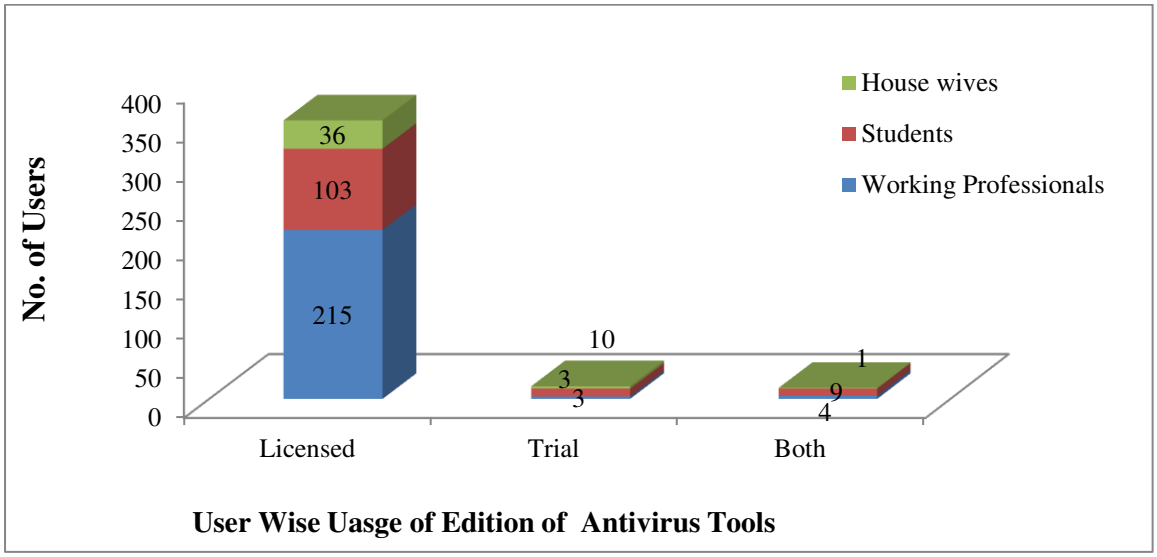
which 1.04 percent are working professionals followed by 2.35 percent are students and only 0.26 percent are house wives.

Table No.4.11: User Wise Usage of Edition of Antivirus tools

Type of User	Licensed	Trial	Both	Total
Working Professionals	215(55.99)	3(0.78)	4(01.04)	222(57.81)
Students	103(26.82)	10(02.60)	9(02.35)	125(31.77)
House wives	36(09.38)	3(00.78)	1(00.26)	37(10.42)
Total	354(92.19)	16(04.16)	14(03.65)	384(100.00)

Figures in bracket indicates Percentage

Graph 4.7: User Wise Usage of type of Anti-virus tools package used



User Wise Uasge of Edition of Antivirus Tools

As can be observed from Graph 4.7, most of the user's use licensed edition of antivirus tools followed by trial and both the editions. Working professionals are highly aware about security and due to that they mostly preferred licensed edition of antivirus tools followed by students. Response from housewives is very low as compared to the working professionals and students regarding usage of licensed edition of antivirus tool.

4.6.3 Usage of Antivirus Tools

Table No. 4.12 shows the usage of Antivirus tools used by the user. Number of antivirus tools are available in the market, due to time period concern, researcher has

considered only six antivirus tools for the study purpose like Quick Heal, McAfee, Kaspersky, Norton and AVG.

It shows that out of 384 users, 58.33 percent user's uses Quick Heal Antivirus tool for their personal computer. As a quick heal is strongest antivirus tools as compared to other antivirus tools. Followed by 50.26 percent user's uses Net Protector antivirus tools, 20.05 percent uses McAfee. Further 18.49 percent user's uses Kaspersky , 14.06 percent user's uses Norton antivirus tool and only 13.02 percent user's uses AVG antivirus tools. Hence it is clear most of the users are in favor of Quick Heal antivirus tool in terms of security reason.

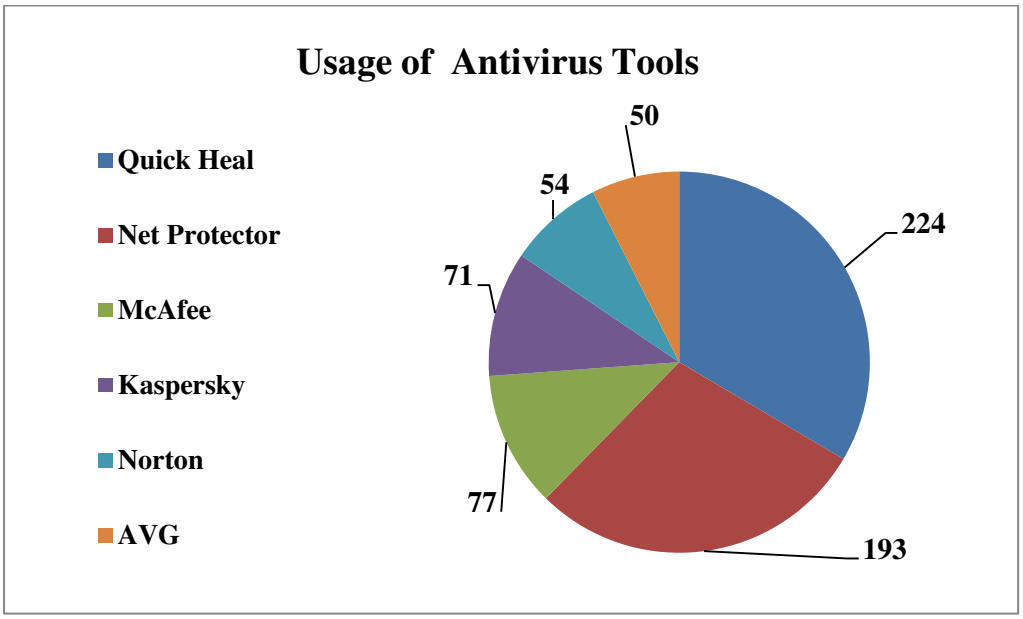
According to users ranking first rank goes to Quick Heal Antivirus tool followed by second to Net Protector, third is McAfee, fourth is for Kaspersky, fifth is for Norton and last one means sixth is AVG antivirus tools.

Table No.4.12: Usage of Antivirus Tools

Usage of Antivirus Tools	No. of Users	Rank
Quick Heal	224(58.33)	1
Net Protector	193(50.26)	2
McAfee	77(20.05)	3
Kaspersky	71(18.49)	4
Norton	54(14.06)	5
AVG	50(13.02)	6

Figures in bracket indicates Percentage

Graph 4.8: Usage of Antivirus Tools



The Pie chart 4.8 indicating the fact of usage of various Antivirus Tools. Most of the users uses Quick heal antivirus tools followed by Net Protector, McAfee, Kaspersky, Norton and AVG.

It is seen that 58.33 percent users prefer to use Quick Heal antivirus tool as a high security reason as compared to the other antivirus tools. Hence this data supports the second objective of the study that identification of the usage of antivirus tools among the users and quick heal is highly used tool among the user.

4.6.4 User wise usage of Antivirus Tools

As per the study purpose, primary data is collected from various types of users like working professionals, students and housewives. Most of the working professionals are used computer on daily basis so for security purpose they required to use any antivirus tools and secure their data. Now a day's student also using their personal computers for study purpose and they also threaten about their study material and started usage of antivirus tools. Followed by housewives, those are also aware about usage os antivirus tools.

Following Table No. 4.13 shows that user wise usage of antivirus tools. It clears that 58.33 percent users use quick heal antivirus tool for security purpose. Out of which

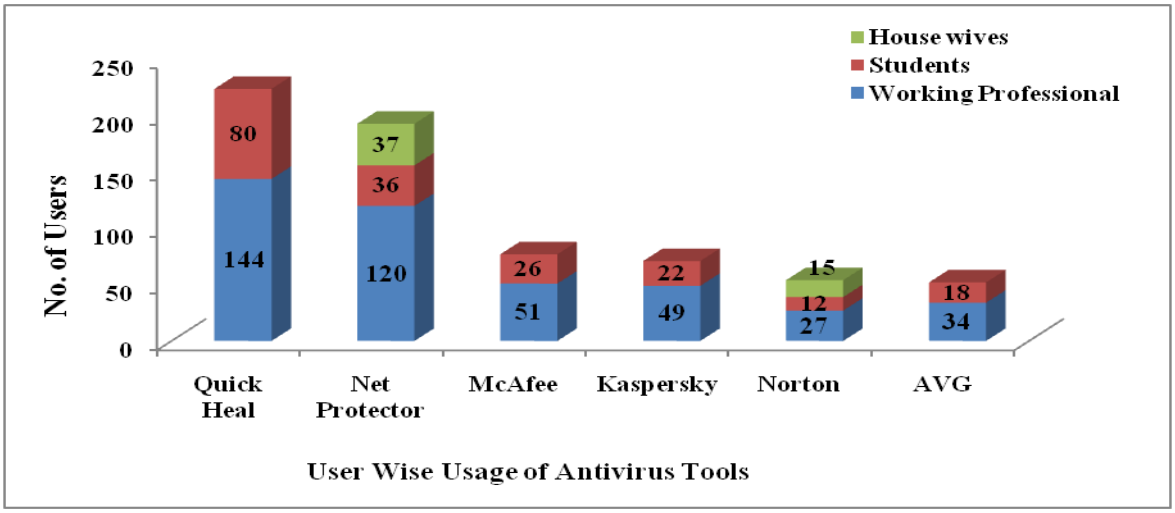
37.50 percents are working professional followed by 20.83 percent students and further no one from housewives category uses quick heal. 50.26 percent users uses Net Protector antivirus tool, out of which 31.25 percent are working professionals, 9.38 percent are students and 9.64 percent are housewives. Whereas 20.05 percent users uses McAfee antivirus tool, out of which 13.28 percent are working professionals, 6.77 percent are students and again no one from house wives category. It has been observes that 18.49 percent users uses Kaspersky antivirus tool which includes 12.76 percent working professionals, 5.73 percent students and no one from house wives category. Also only 14.06 percent users uses Norton antivirus tools, out of which 7.03 percent are woking professionals followed by 3.13 percent are students and only 3.91 percent are house wives. Also 13.02 percent users uses AVG antivirus tool which includes 8.85 percent are working professionals and 4.16 percent are students.

Table No.4.13: User wise usage of antivirus Tools

Usage of Antivirus Tools	Working Professional	Students	House wives	Total
Quick Heal	144(37.50)	80(20.83)	0(00.00)	224(58.33)
Net Protector	120(31.25)	36(09.38)	37(09.64)	193(50.26)
McAfee	51(13.28)	26(06.77)	0(00.00)	77(20.05)
Kaspersky	49(12.76)	22(05.73)	0(00.00)	71(18.49)
Norton	27(07.03)	12(03.13)	15(03.91)	54(14.06)
AVG	34(08.85)	16(04.16)	0(00.00)	50(13.02)

Figures in bracket indicates Percentage

Graph 4.9: User wise usage of antivirus Tools



Graph 4.9 shows user wise usage of antivirus tools. It is seen that, most of the users preferred to use Quick heal antivirus tools followed by Net Protector, McAfee, Kaspersky, Norton and AVG. In between it is observed that most of the working professionals and students are highly used antivirus tools for security reason whereas house wives use only Net Protector and Norton Antivirus tool as compared to other tools.

4.6.5 Cost of Antivirus Tool

In today's world, User wants higher security by paying less cost but some users focus on security of their data instead of cost which they have to pay. From these it clears that users are very much concerned about security and for that purpose need to study about various slabs of cost which have to pay while purchasing antivirus tools.

Table No. 4.14 shows the ratio of user along with range of cost of antivirus tools purchased. From this table, it clears that 55.70 percent users prefer antivirus tool with cost less than Rs. 1000/- whereas 28.50 percent users look for Rs. 1001/- to Rs. 1500/- . Only 8.30 percent users prefers cost of antivirus tool in between range from Rs. 1501/- to Rs. 2000/- further only a few like 1.80 percent users prefer cost amount of Rs.2000/- to Rs. 2500/- and further 5.70 percent users ready to pay cost more than Rs. 2500/-

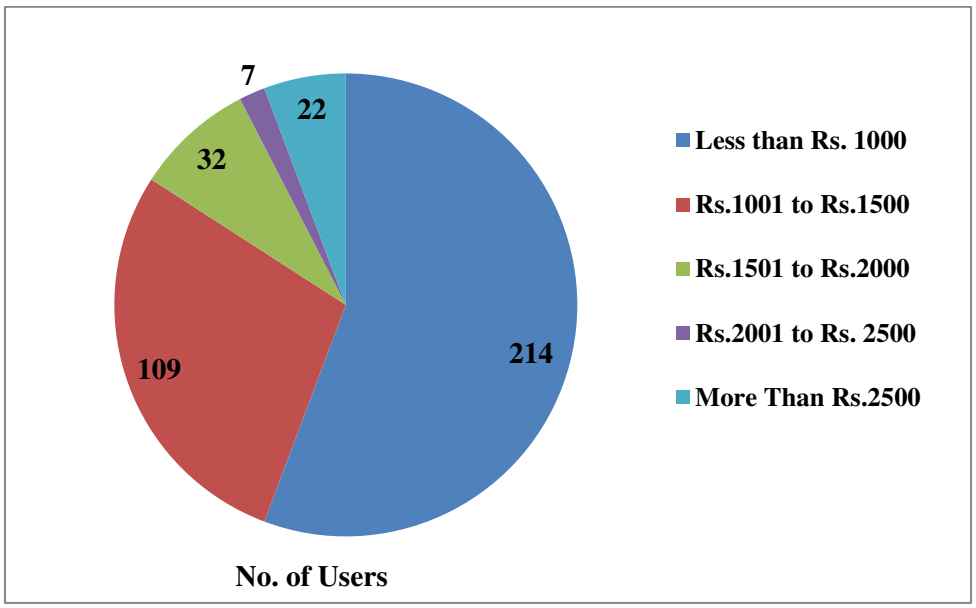
Table No.4.14: Cost of Antivirus Tool

Cost of antivirus tools purchased	No. of Users
Less than Rs. 1000	214(55.70)
Rs.1001 to Rs.1500	109(28.40)
Rs.1501 to Rs.2000	32(08.30)
Rs.2001 to Rs. 2500	7(01.80)
More Than Rs.2500	22(05.70)
Total	384(100.00)

Figures in bracket indicates Percentage

Following Graph 4.10 shows the cost of antivirus tools preferred by the user against security of their personal computers. From graph, it is seen that most of the users prefers the cost of antivirus tools should be less than Rs. 1000/- followed by cost of range in between Rs. 10001/-to Rs. 1500/- and further range in between Rs.1501/- to Rs. 2000/-. It is also seen that only a few users prefer amount of Rs. 2001/- to Rs. 2500/- and more than Rs. 2500/-. So it clears that user wants best security in less cost.

Graph 4.10: cost of anti-virus



4.6.6 : Selection of antivirus tools by user with respect to Cost

As a part of study, need to identify selection of antivirus tools by various types of users with respect to cost. Generally most of the users want higher security in lower cost. So as per the number of antivirus tools and with respect to their cost, primary data has been collected.

Table 4.15 shows the Selection of antivirus tools by user with respect to Cost. It is seen that 55.70 percent users prefer to purchase antivirus with amount less that Rs. 1000/-, out of which 13.02 percent user prefers purchase of Quick Heal, 25 percent purchase Net Protector, 7.03 percent purchase McAfee, 3.65 percent purchase Kaspersky, 3.91 percent purchase Norton and only 3.13 purchase AVG.

It is followed by 28.40 percent users purchase antivirus tools in between range of Cost of Rs. 1001/- to Rs. 1500/-, out of which 11.72 percent user prefers purchase of Quick Heal, 7.29 percent purchase Net Protector, 2.86 percent purchase McAfee, 2.34 percent purchase Kaspersky and a few 2.08 percent purchase Norton & AVG.

Further 8.30 percent users purchase antivirus tools in between range of Cost of Rs. 1501/- to Rs. 2000/-, out of which 3.13 percent user prefers purchase of Quick Heal, 1.30 percent purchase Net Protector & McAfee, 1.04 percent purchase Kaspersky & AVG and a few 0.52 percent purchase Norton .

It is also observed that only 1.82 percent users purchase Quick Heal and no one from other categories of antivirus tools from cost range in between Rs.2001/- to Rs. 2500/-.

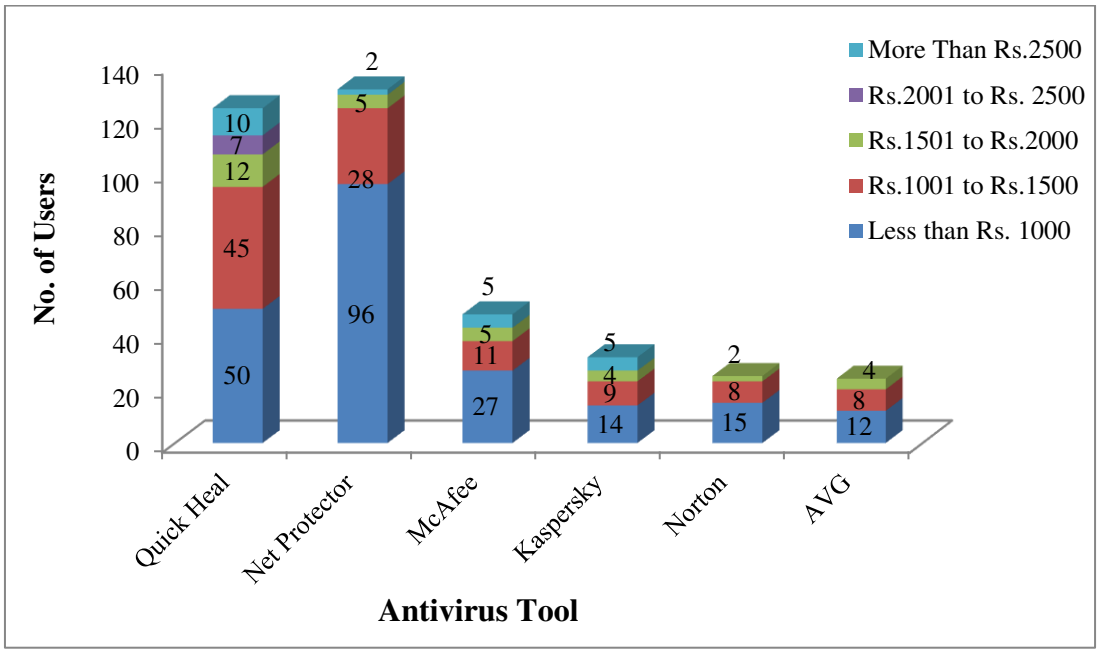
Also 5.70 percent users purchase Antivirus tools with cost more than Rs. 2500/-, out of which 2.60 percent users purchase Quick Heal, a few 0.52 percent users purchase Net Protector,1.30 percent users purchase McAfee & Kaspersky and no one purchase Norton & AVG.

Table No.4.15: Selection of antivirus tools with respect to Cost

Antivirus Tools	Cost range of Antivirus Tools					Total
	Less than Rs. 1000	Rs.1001 to Rs.1500	Rs.1501 to Rs.2000	Rs.2001 to Rs. 2500	More Than Rs.2500	
Quick Heal	50(13.02)	45(11.72)	12(03.13)	7(01.82)	10(02.60)	124(32.29)
Net Protector	96(25.00)	28(07.29)	5(01.30)	0(00.00)	2(00.52)	131(34.11)
McAfee	27(07.03)	11(02.86)	5(01.30)	0(00.00)	5(01.30)	48(12.50)
Kaspersky	14(03.65)	9(02.34)	4(01.04)	0(00.00)	5(01.30)	32(08.33)
Norton	15(03.91)	8(02.08)	2(00.52)	0(00.00)	0(00.00)	25(06.51)
AVG	12(03.13)	8(02.08)	4(01.04)	0(00.00)	0(00.00)	24(06.25)
Total	214(55.70)	109(28.40)	32(08.30)	7(01.82)	22(05.70)	384(100.00)

Figures in bracket indicates Percentage

Graph.4.11: Selection of antivirus tools with respect to Cost



Graph 4.11 shows the Selection of antivirus tools by user with respect to Cost. It is clear that most of the users purchase Net Protector with cost less than Rs. 1000/- followed by Quick Heal, McAfee, Kaspersky, Norton & AVG.

But in range of cost Rs. 1001/- to Rs. 1500/- and Rs.1500/- to Rs.2000**/-,** most of the users purchase Quick Heal followed by Net Protector, McAfee, Kaspersky and Norton & AVG.

In between range Rs.2001/- to Rs. 2500/-, users only purchase Quick Heal not any other antivirus tools. Whereas cost more than Rs.2500/-, users purchase only Quick Heal, Net Protector, McAfee & Kaspersky but not Norton and AVG.

4.6.7 Type of Antivirus tools installed Personal Computer

Antivirus products are categorized into three parts such as Internet Security [IS], Total Security [TS], and Antivirus [AV]. Antivirus: products are the products, which are primarily focused on detecting and remediation viruses and Spyware. Internet Security product provides all the virus and Spyware removal features of an AV, as well as extra functions to provide greater Internet protection. These features may include protection against phishing, root kit detection, firewalls and scanning of web pages and HTTP data. Total Security: products provide data migration and backup features on top of all security features common to IS products (Paul Royal) with mobile security, safe banking and parental control.

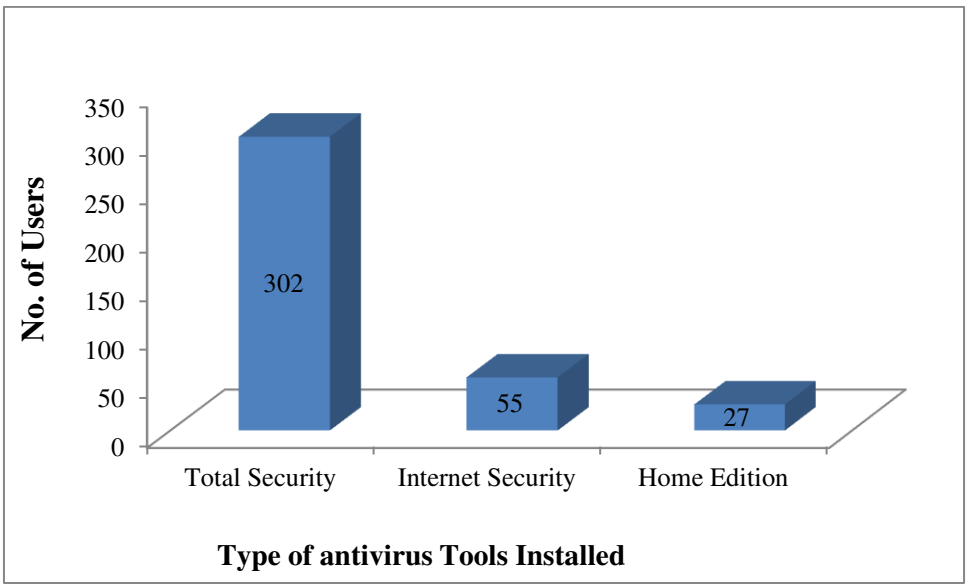
Following Table 4.16 shows the type of antivirus tools installed on personal computer. As per the primary data, 78.64 percent users installed total security antivirus tool followed by 14.30 percent users used internet security antivirus tools and further only 7 percent users using home edition.

Table No.4.16: Type of Antivirus tools installed

Type of Antivirus tools installed on Personal Computer	No. of Users
Total Security	302(78.64)
Internet Security	55(14.30)
Home Edition	27(07.00)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.12: Type of Antivirus tools installed on Personal Computer



Following Graph 4.12 shows the type of antivirus tools installed by users on his/her personal computer. It is seen that most of the users prefers to use total security antivirus tool as compared to the internet security and home edition.

4.6.8 User wise Installation of Antivirus Tools

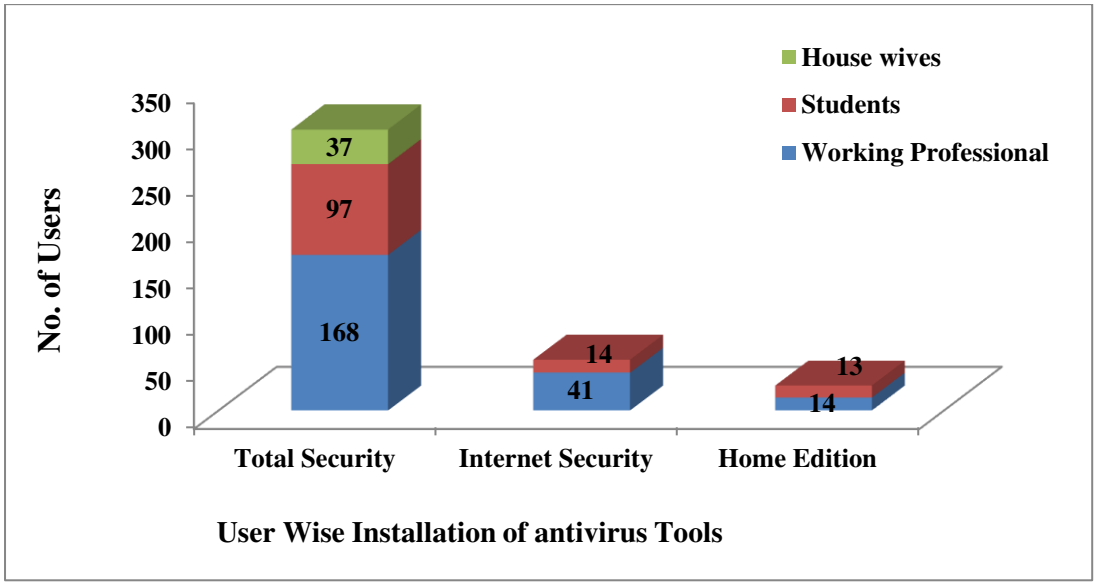
As above table shows the type of antivirus tools installed on personal computer. As three types of users considered for study purpose, so need to study user wise installation of antivirus tools. Following Table 4.17 shows that user wise installation of antivirus tools on users computer. It is observed that 58.07 percent working professionals installed antivirus tools on their personal computers out of which 43.75 percent users installed total security followed by 10.68 percent users installed internet security and 3.65 percent users installed home edition on their personal computers. It is also observed that 32.29 percent students installed antivirus tool on their personal computer, out of which 25.26 percent users installed total security, 3.65 percent users installed internet security and only a few 3.39 percent users installed home edition. Further only 9.64 housewives installed antivirus tool on their personal computer, out of which 9.64 percent house wives installed total security antivirus tool. It is also seen that house wives haven't installed internet security and also home edition antivirus tool on their personal computers.

Table No.4.17: User wise Installation of Antivirus Tools

User type	Type of antivirus tools installed			Total
	Total Security	Internet Security	Home Edition	
Working Professional	168(43.75)	41(10.68)	14(03.65)	223(58.07)
Students	97(25.26)	14(03.65)	13(03.39)	124(32.29)
House wives	37(09.64)	0(00.00)	0(00.00)	37(09.64)
Total	302(78.65)	55(14.32)	27(07.03)	384(100.00)

Figures in bracket indicates Percentage

Graph 4.13: User wise Installation of Antivirus Tools



Graph 4.13 shows the User wise Installation of Antivirus Tools on personal computers of various types of users. It is seen that working professionals and students are highly used total security antivirus tool on their personal computer followed by internet security and home edition. Only a few house wives used only total security not a internet security and home edition. So it clears that ratio of usage of total security among working professionals followed by students is very high as compared to the house wives. Usage of internet security and home edition among house wives is absolutely not any.

4.6.9 Summary

It is seen that most of the users prefer to use quick heal antivirus tool followed by Net Protector, McAfee, Kaspersky, Norton and AVG. Also they prefers the licensed edition and Total Security type of antivirus tool as compared to the free/trial edition and Internet Security and Home Edition. In term of cost, user prefers purchase of Antivirus tool with cost less than Rs.1000/- as compared to other range of cost.

4.6.9 Frequency of Update and Scanning of Antivirus Tools

To check and measure security performance of antivirus tool, it is need to update antivirus tool on regular basis and do the scanning of personal computer. So user will get the idea of threats and virus attacks and they will try to minimize threats and reduce risk at lower level by choosing right antivirus tool.

Following Table No. 4.18 shows Frequency of Update and Scanning of Antivirus Tools by the users. It is seen that 63.30 percents users said that updating of antivirus tool done automatically and 53.40 percent users said that full system scan done automatically. Whereas 4.70 percent users updates antivirus tool daily and 10.20 percent users does the full systems scan daily. 7.80 percent users update antivirus tool and 19.30 percent users do the full system scan at least once in a week. Whereas 18.80 percent users update antivirus tool and 4.90 percent users do the full systems scan at least once in a month.

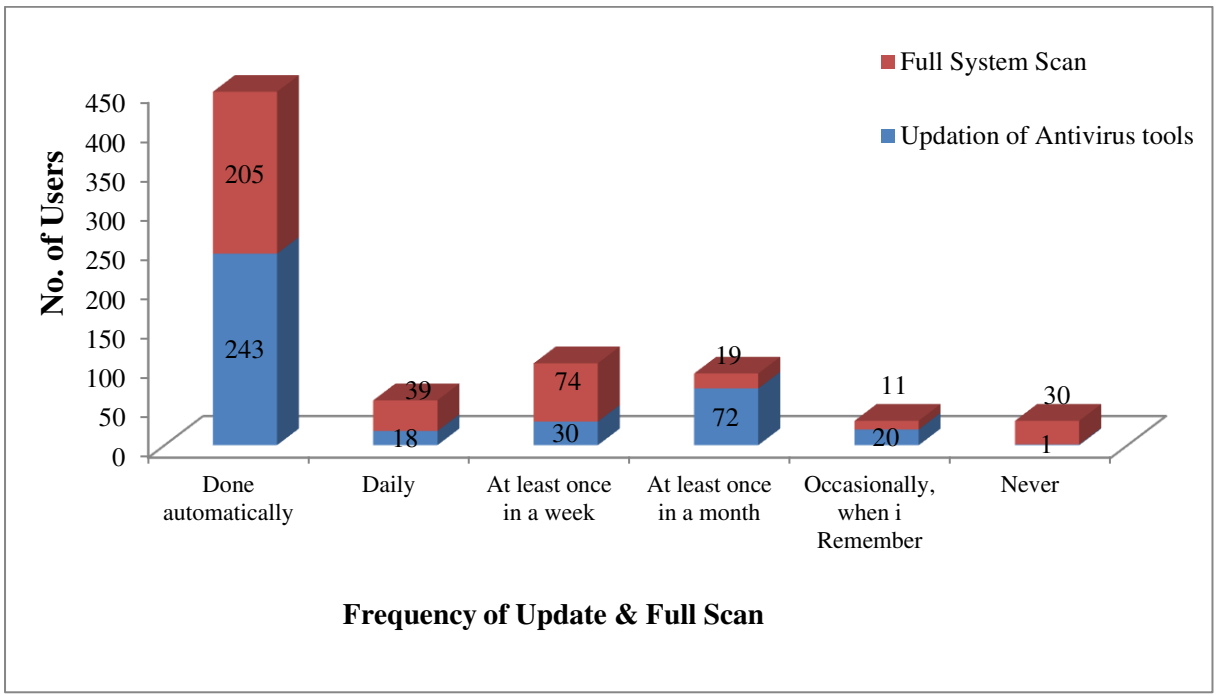
Further a very few that is 5.20 percent users update antivirus toll occasionally when they remember and 2.90 percent users do the full system scan Occasionally when they remember. It is also observed that only 0.30 percent users not dong updating of antivirus tool and 7.80 users not scanning full system.

Table No. 4.18: Frequency of Update and Scanning of Antivirus Tools

Frequency of Update and Scanning of Antivirus Tools	No. of Users who update antivirus tools	No. of Users who scanning antivirus tools(Full System)
Done automatically	243 (63.30)	205(53.40)
Daily	18(04.70)	39(10.20)
At least once in a week	30(07.80)	74(19.30)
At least once in a month	72(18.80)	19(04.90)
Occasionally, when I Remember	20(05.20)	11(02.90)
Never	1(00.30)	30(07.80)
Total	384(100.00)	384(100.00)

Figures in bracket indicates Percentage

Graph 4.14: Frequency of Update and Scanning of Antivirus Tools



Frequency of Update & Full Scan

Graph 4.14 shows the Frequency of Update and Scanning of Antivirus Tools by the users. It is observed that most of the users depend on automatic updating and scanning of antivirus tool when they start their personal computer.

It is also observed that most of the users update antivirus tool at least once in a month followed by at least once in a week, occasionally when they remember, daily and then no updation. Whereas about scanning of full system scan, users does the full system scan of personal computer at least once in a week followed by daily, never does the scanning, at least once in a month and Occasionally when they remember.

It is clear that ratio of updation of antivirus tool is little bit higher than of scanning of full system. But around 7.80 percent users not doing the full scanning of their personal computer whereas a only a few that is 0.30 percent users not doing updation of their personal computers..

4.6.10 Version of Antivirus Tool installed on personal computer

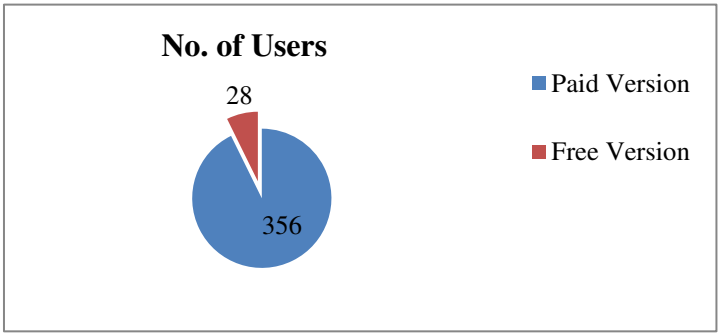
Most of the users look at the cost while purchasing of antivirus tools, so need to identify how many users prefers paid and free version of antivirus tool. Following Table No. 4.19 shows the status of antivirus tool version installed on user's personal computer. It clears that 92.70 percent users used paid version whereas only a few that is 7.30 percent users used free version of antivirus tool.

Table No. 4.19: Version of Antivirus Tool installed on personal computer

version of antivirus tools used	No. of Users
Paid Version	356(92.70)
Free Version	28(07.30)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.15: Version of Antivirus Tool installed on personal computer of users



Above Graph 4.15 shows the version of antivirus tools installed on users personal computer. For graph it clears that ratio of paid version users is higher than that of free versions. Hence we can say that most of the users are highly aware of their data and its security and due to that reason using paid version instead of free version of antivirus tools.

4.6.11 Financial transaction through personal computer

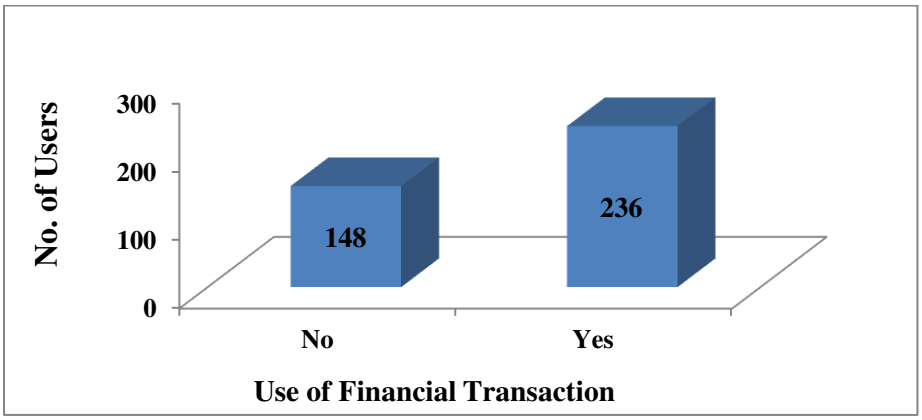
In today's IT world , most of the user avoid to go bank for financial transaction and due to that reason they uses online banking for their regular financial transaction and due to which they think that they will save their time , effort and travelling cost also. But while during online banking transaction they should be aware about threats which will attack during banking transaction, misuse of their passwords, card numbers etc. So there is need to identify how many users do the financial transaction online and how they maintained security. Following Table No. 4.20 shows the number of users doing financial transactions by using their personal computer. It is observed that 61.50 percent users doing financial transactions by using their personal computer whereas 38.50 percent users not doing financial transaction by using their personal computer.

Table No.4.20: Financial Transaction through Personal Computer

Financial Transaction through Personal Computer	No. of Users
Yes	236(61.50)
No	148(38.50)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.16: Financial Transaction through Personal Computer



Above Graph 4.16 shows the number of users doing financial transactions by using

their personal computer. It is seen that most of the users are doing digital financial transactions shows that net banking in India is growing.

4.6.12 Financial Loss before usage of Antivirus Tools

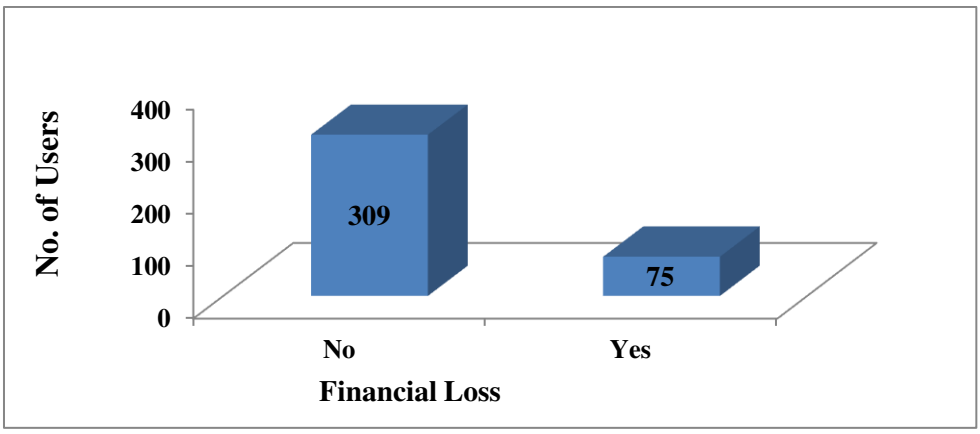
As Table No. 4.20 shows the number of users doing financial transactions by using their personal computer, so need to identify status of Financial Loss before usage of Antivirus Tools. Following Table No. 4.21 shows the status of Financial Loss before usage of Antivirus Tools. It is observed that 80.46 percent users have not faced any financial loss but a 19.56 percent user has financial loss due to virus before using of antivirus tools.

Table No.4.21: Financial Loss before usage of Antivirus Tools

Financial Loss before usage of antivirus tool	No. of Users
No	309(80.46)
Yes	75(19.54)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.17: Financial Loss before usage of Antivirus Tools



Graph 4.17 shows the status of financial loss before using antivirus tool. It is clear that ratio of financial loss is very low and it clears that might be users are not aware about threats and while during financial transaction they need to check for secure

website like https:/ instead of http:/ only. So here we can say that awareness regarding security among the user is high.

4.6.13 Imposition of restrictions by the user to avoid virus attack

As Table No. 4.21 shows the status of Financial Loss before usage of Antivirus Tools and from it is observed that around 20 percent users has the financial loss before using antivirus tool so need to identify imposition of restrictions by the user to avoid such type of attacks.

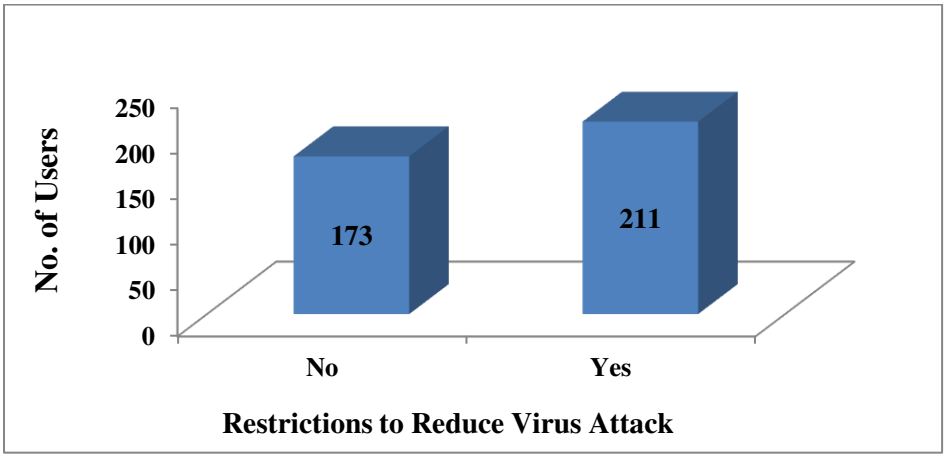
So as per the study requirement, primary data is collected from users. Following Table No.4.22 shows the Imposition of restrictions done by the user to avoid virus attack. It is seen that around 54.90 percent users imposed restrictions such as blocking of pendrive, open the bank site by typing of bank url in browser, always use https web site showing padlock symbol. Whereas 45.10 percent users has not imposed any restrictions.

Table No.4.22: Imposition of restrictions done by the user to avoid virus attack

Imposition of restrictions on the user to avoid virus attack	No. of Users
Yes	211(54.90)
No	173(45.10)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.18: Imposition of restrictions done by the user to avoid virus attack



Above Graph 4.18 shows the Imposition of restrictions done by the user to avoid virus attack. It is clear that 54.90 percent users are vigilant while remaining users need to learn awareness about threats, attacks related to online banking.

4.6.14 Protection of all your computers / Laptops/mobile phones protected by anti-virus software

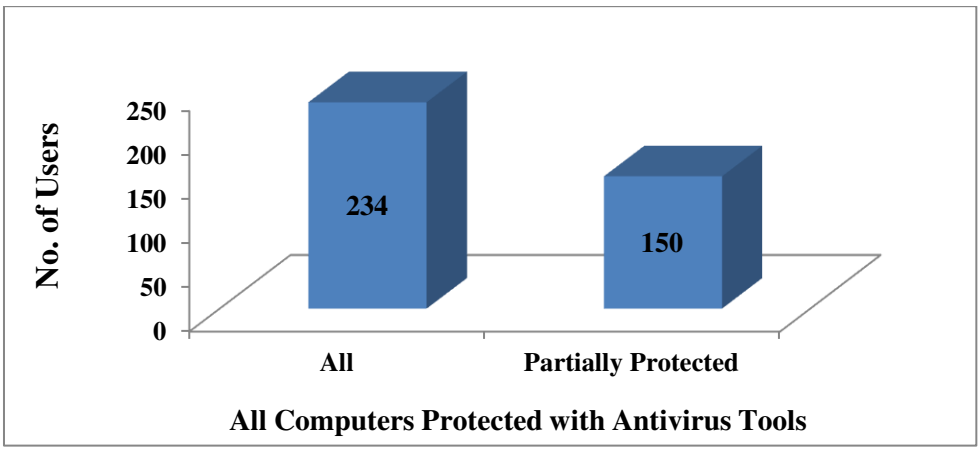
Research is mainly focus on management of antivirus tool by the various types of the users. It is also need of study to identify how many users personal computers/laptops/mobiles are protected by antivirus tools. Following Table No. 4.23 shows the status of Protection of all your computers / Laptops/mobile phones by anti-virus software with respect to the users. It is seen that around 60.90 percent users personal computers/Laptops/Mobile phones are protected with antivirus tools whereas 39.10 percents users personal computers/Laptops/Mobile phones are not protected with antivirus tools

Table No.4.23: Protection of all your computers / Laptops/mobile phones by anti-virus software with respect to the users

Computers Protect With Antivirus Tools	No. of Users
All	234(60.90)
Partially Protected	150(39.10)
Total	384(100.00)

Figures in bracket indicates Percentage

Graph 4.19: Protection of all your computers / Laptops/mobile phones by anti-virus software with respect to the users



Above Graph 4.19 shows that status of Protection of all your computers / Laptops/mobile phones by antivirus tools with respect to the users. It clears that ratio of protection of all your computers /laptops/mobile phones by antivirus tool with respect to the users are high as compared to the partially protected with antivirus tools. So we can conclude that most of the users are aware about protection of their personal computers/Laptops/Mobile phones and accordingly they take care of all devices. But for remaining users it is required to create awareness regarding protection of all devices connected to the personal computer they are using because one compromised device can be gateway into your entire home network resulting to the infection of computers and cellular phones and more.

4.6.15 To study the services provided by the antivirus company

An attempt was made to meet the sixth objective "To study the services provided by the antivirus company". The primary data collected from the antivirus users fulfilled it. Table No. 4.24 shows the various parameters of status of present antivirus tools for assessment Service provided by the help/support center, Procedure of Virus Database Definition Update and Procedure of Version Update and their rank. To meet the objective question is designed by using various parameters which defines the status of antivirus tools.

It is observed that for each parameter average scale is in-between 1 to 5 that is in-between Excellent to Poor. In fact all are around 4 which mean that with respect to all the parameters much improvement is observed.

It is seen that highest average value is 4.03 for Service provided by the help/support center followed by Procedure of Virus Database Definition Update is and Procedure of Version Update is 4.00. All these three indicate the status of the present antivirus tools used by the user and moreover due to support of service provider, virus database and version are very much satisfied to the user.

Table No.4.24 also shows the ranks of each parameter used for assessment status of the present antivirus tools used by the user. Based on primary data, users are satisfies with help /support provided by the service provider and it got *First* rank with weightage of 72.13 percent. It is followed by *Second* rank for 'Virus Database Definition update' with weightage of 70.57 percent. Finally Third rank is for

'Procedure of Version Update' with weightage of 65.36 percent. According to tshese it clear, users are very much satisfied with present antivirus tools which they are using. This proves that antivirus companies are also taking reactive efforts from their side by providing prompt service for definitions of unseen viruses and facility of virus database definition update as well as version update.

Table No.4.24: Status of services provided by the antivirus company

Antivirus Tools	Excellent [5]	Very Good[4]	Good [3]	Fair [2]	Poor [1]	Total	Avg. Value	Rank
Service provided by the help/support center	129 (33.59)	148 (38.54)	99 (25.78)	7 (01.82)	1 (00.26)	384	4.03	1
Procedure of Virus Database Definition Update	128 (33.33)	143 (36.72)	98(26.82)	14 (03.65)	1 (00.26)	384	4.00	2
Procedure of Version Update	145 (37.76)	106 (27.60)	121 (31.51)	12 (03.13)	0 (00.00)	384	4.00	3

Figures in bracket indicates Percentage

Note: Average Scale 1 to 5 (where Excellent=5;Very Good=4;Good=3;Fair=2 & Poor=1)

4.6.16 Services provided by the antivirus company's support/help center

An attempt is made to meet the seventh objective "To study the services provided by the antivirus company's support/help center." The primary data collected from user's of antivirus company has fulfilled it. Table No. 4.25 shows the various parameters of technical supports of present antivirus tools for assessment like online support, support through email, telephonic support, user forum and user manual/trouble shooting manual and their rank. To meet the objective question is designed by using various parameters which defines the status of antivirus tools.

It is observed that for each parameter average scale is in-between 1 to 5 that is in-between Excellent to Poor. In fact all are around 4 which mean that with respect to all the parameters much improvement is observed.

It is seen that highest average value is 4.16 for 'Online Support' followed by 'Supprt through email with average value is 4.11, for 'telephonic support' with average value is 4.04, for user forum average value is 4.02 and further for User manual / Trouble hooting manual is 4.01. All these five indicate the support by antivirus company is good to the user of the present antivirus and moreover due to support of service provider most of the user are very much satisfied to the user.

Table No.4.25 also shows the ranks of each parameter used for assessment status of the present antivirus tools used by the user. Based on primary data, users are satisfies with 'online support' and it got *First* rank with weightage of 76.04 percent. It is followed by *Second* rank for 'Support through email' with weightage of 80.99 percent. Third rank is for 'Telephonic support' with weightage of 74.48 percent. Finally Second last rank is for 'User Forum' with weightage of 75.78 percent. Further last rank is for 'User manual / Trouble hooting manual' with weightage of 75.52 percent. According to these it clear, users are very much satisfied with present antivirus tools which they are using and support provided by the antivirus company.

Table No.4.25: Services provided by the antivirus company's support/help center

Aspects related to the technical support	Excellent [5]	Very Good[4]	Good [3]	Fair [2]	Poor [1]	Total	Avg. Value	Rank
Online support	177 (46.09)	115 (29.95)	69 (17.97)	22 (05.73)	1 (00.26)	384	4.16	1
Support through Email	151 (39.32)	160 (41.67)	50 (13.02)	11 (02.86)	12 (03.13)	384	4.11	2
Telephonic support	138 (35.94)	148 (38.54)	75 (19.53)	22 (05.73)	1 (00.26	384	4.04	3
User Forum	128 (33.33)	163 (42.45)	68 (17.71)	23 (05.99)	2 (00.52)	384	4.02	4

User manual / Trouble hooting manual	123 (32.03)	167 (43.49)	71 (18.49)	21 (05.47)	2 (00.52)	384	4.01	5

Figures in bracket indicates Percentage

Note: Average Scale 1 to 5 (where Excellent=5;Very Good=4;Good=3;Fair=2 & Poor=1)

4.6.17 Scanning capability of the present Antivirus Tool

To measure the quality and performance of present antivirus tool, there is need to check scanning capability of the present antivirus tool. So user get the idea about scanning capability of antivirus tool. An attempt is made to assess the scanning capability of antivirus tool by putting some observations regarding various parameters of scaning and its capability to identification of threats.

Table No. 4.26 shows the various parameters of Scanning capability of the present Antivirus Tool. To meet the objective question is designed by using various parameters which defines the scanning capability of current antivirus tool. (Para 5.6.1). It is observed that for each parameter average scale is in-between 1 to 5 that is in-between Excellent to poor. In fact all are above 3.5 which mean that with respect to all the parameters much improvement is observed.

It is seen that highest average value is 4.24 on-access scanning followed by scheduled scanning is 4.08 and compressed files scanning is 3.92. All these four indicate that scanning capability of present antivirus tool is high and users are very much satisfies with present antivirus tool.

Apart from these benefits it is observed that average value foe registry startup protection is 3.90 followed by 3.89 for manual scanning 3.88 for email protection,3.87 for quarantines infected files,3.85 for on-demand scanning, 3.84 for web mail protection, 3.83 for Auto-Clean infected files. Further also average value for ad ware/Spyware scanning is 3.73, 3.62 is for file sharing, 3.56 is for Heuristic scanning whereas 3.52 is for Script blocking and further 3.51 for instant messaging protection.

Table No.4.26: Scanning capability of the present Antivirus Tool

Aspects related to the scanning capability	**Excellent [5]**	**Very Good [4]**	**Good [3]**	**Fair[2]**	**Poor [1]**	**Total**	**Avg. Value**	**Rank**
On-access Scanning	190 (49.80)	109 (28.39)	74 (19.27)	11 (02.86)	0 (00.00)	384	4.24	1
Scheduled Scanning	150 (39.06)	135 (35.16)	87 (22.66)	5 (01.30)	7 (01.82)	384	4.08	2
Compressed Files Scanning	145 (37.76)	100 (26.04)	102 (26.56)	37 (09.64)	0 (00.00)	384	3.92	3
Registry Startup Protection	130 (33.85)	126 (32.81)	94 (24.48)	26 (06.77)	8 (02.08)	384	3.90	4
Manual Scanning	119 (30.99)	124 (32.29)	121 (31.51)	20 (05.21)	0 (00.00)	384	3.89	5
Email protection	121 (31.51)	143 (37.24)	88 (22.92)	17 (04.43)	15 (03.91)	384	3.88	6
Quarantines Infected Files	115 (29.95)	144 (37.50)	92 (23.96)	25 (06.51)	8 (02.08)	384	3.87	7
On-demand Scanning	106 (27.60)	128 (33.33)	137 (35.68)	13 (03.39)	0 (00.00)	384	3.85	8
Web Mail protection	137 (35.68)	97 (25.26)	110 (28.65)	32 (08.33)	8 (02.08)	384	3.84	9
Auto-Clean Infected Files	115 (29.95)	133 (34.64)	104 (27.08)	18 (04.69)	14 (03.65)	384	3.83	10
Ad ware / Spyware scanning	108 (28.13)	107 (27.86)	126 (32.81)	43 (11.20)	0 (00.00)	384	3.73	11
File Sharing protection	94 (24.48)	99 (25.78)	150 (39.06)	33 08.59)	8 (02.08)	384	3.62	12

Heuristic Scanning	75 (19.53)	117 (30.47)	148 (38.54)	36 (09.38)	8 (02.08)	384	3.56	13
Script Blocking	77 (20.05)	127 (33.07)	119 (30.99)	40 (10.42)	21 (05.47)	384	3.52	14
Instant Messaging protection	78 (20.31)	111 (28.91)	145 (37.76)	27 (07.03)	23 (05.99)	384	3.51	15

Figures in bracket indicates Percentage

Note: Average Scale 1 to 5 (where Excellent=5;Very Good=4;Good=3;Fair=2 & Poor=1)

It is seen that first rank is for on-access scanning followed by second rank is for scheduled scanning and third rank is for compressed files. Further fourth rank is for registry startup protection, fifth rank is for manual scanning, sixth rank is for email protection, seventh rank is for quarantines infected files and eighth rank is for on-demand scanning. Also further ninth rank is for web mail protection followed by tenth rank is for Auto-Clean infected files, eleventh rank is for ad ware/Spyware scanning, twelve rank is for file sharing, thirteenth rank is for Heuristic scanning whereas fourteenth rank is for Script blocking and last means fifteenth rank is for instant messaging protection.

4.6.18(A) Management Antivirus Tool by the User

While using antivirus tool, user have to do setting of antivirus tool to keep it up to date. An attempt is made to study the various setting of present antivirus tools by the user. Table No. 4.27 shows the various parameters of settings of antivirus tools done by the user.

It includes that parameter like, On Scan Scheduling, Password Protect Settings, Parental Control, Files and Folders, External drivers and devices, Internet & Network and Emails. To meet the objective question is designed by using various parameters which defines the settings of antivirus tools.

Scan scheduling setting is used to schedule the whole system scan including RAM (Random access memory), boot scan, registry scan) according to the user's convenient date or time.

In parental control settings in antivirus tool allows to ensure children's online safety. In this the user has to create a separate standard user account to configure the settings in which every user can block access of child to website categories (chat, adult, violence, movies, games) and also schedule the internet access time of child.

In files and folder settings users can provide settings related to blocking suspicious files, rogue ware scanning, anti key logging (preventing sending information typed with keyboard of your PC to hackers), quarantine and backup settings. In this users can also select the action to be taken when the virus is found. Here user can select repair, delete or deny access option.

In external drives and device settings users can disable auto run of external drives like usb drives, CD/DVDs etc, scan external drives as soon as they are connected, blocks external drives like CD/DVDS and also scan mobile automatically when connected.

In internet and network settings user can configure firewall protection (protection from incoming data), browsing protection (blocks access to infected sites), malware protection (protects pc from spyware, adware, key loggers and risk ware), phishing protection, browser sandbox (ensures privacy and additional security while surfing), safe banking , IDS /IPS (detects and prevents intrusion attempts).

In email settings users can set automatic protection against malwares coming through emails, allows only trusted email clients to send email and blocks spam (unwanted emails like phishing and porn emails).

It is observed that for each parameter average scale is in-between 1 to 3 that is in-between satisfactory to Non-satisfactory. In fact all are more than 2.5 which mean that with respect to all the parameters much improvement is observed.

It is seen that highest average value is 2.83 for 'On Scan reporting/History' followed by 'External drivers and devices' and Internet & Network'. Also average value of 'emails' is 2.74, followed by 'Password Protect settings' with average value is 2.71, for 'Files & Folders' is 2.70 and further for 'parental control' with average value is

2.44. All these seven indicate the setting status of the present antivirus tool to the user .

Table No.4.27: Management Antivirus Tool by the User

Types of Setting	Satisfactory	Can't Say	Not Satisfactory	Average Value
Scan scheduling	328(85.42)	47(12.24)	9(02.34)	2.83
Internet and network	320(83.33)	64(16.67)	0(00.00)	2.83
External drives and devices	320(83.33)	64(16.67)	0(00.00)	2.83
Emails	302(78.65)	64(16.67)	18(04.69)	2.74
Password Protect Settings	296(77.21)	66(17.19)	21(05.60)	2.71
Files and folders	288(75.00)	77(20.05)	19(04.95)	2.70
Parental Control	200(52.08)	152(39.58)	32(02.34)	2.44

Figures in bracket indicates Percentage

4.6.19 (B) Frequency of Settings of present Antivirus Tool by the User

Above Table No. 4.27 shows the Settings of present Antivirus Tool by the User. As per primary data and need of study, need to check frequency of setting of antivirus tool done by the user. So various parameters are considered and accordingly various options used for data collection purpose like daily, weekly, monthly, yearly and occasionally. Following Table No.4.28 shows the frequency of settings of present antivirus tool by the user.

It clears that most of the users that is 56.77 percent, tighten the privacy settings of facebook on monthly basis followed by weekly is 19.79 percent, 11.20 percent doing it occasionally whereas 6.51 percent is yearly and 5.73 percent user doing it daily. Ratio of Tightened privacy setting in your facebook monthly is higher than that of daily, weekly, yearly and occasionally.

It clears that most of the users that is 56.77 percent, Change your passwords of net banking on monthly basis followed by weekly is 19.79 percent, 11.20 percent doing it occasionally whereas 6.51 percent is yearly and 5.73 percent user doing it daily. Ratio of Changing passwords monthly of net banking is higher than that of daily, weekly, yearly and occasionally.

It is seen that most of the users that is 52.08 percent, Chang e email password on monthly basis followed by weekly is 21.35 percent, 11.20 percent doing it occasionally whereas 8.59 percent is daily and 6.77 percent user doing it yearly. Ratio of Changing password of email monthly is higher than that of daily, weekly, yearly and occasionally.

Whereas 44.27 percent users take backup of their data occasionally followed by 27.60 percent yearly and 14.06 percent users take backup of data weekly and monthly and further no one take backup of their data on daily basis.

Table No.4.28: Frequency of Settings of present Antivirus Tool by the User

Factor	**Daily**	**Weekly**	**Monthly**	**Yearly**	**Occasionally**
Tightened privacy setting in your facebook	22 (05.73)	76 (19.79)	218 (56.77)	25 (06.51)	43 (11.20)
Change your passwords of net banking	22 (05.73)	76 (19.79)	218 (56.77)	25 (06.51)	43 (11.20)
Change your passwords of email accounts	33 (08.59)	82 (21.35)	200 (52.08)	26 (06.77)	43 (11.20)
Take backup of your data	0	54 (14.06)	54 (14.06)	106 (27.60)	170 (44.27)
Change the security settings of our browser	0	27 (07.03)	44 (11.46)	89 (23.18)	224 (58.33)
Change the security	0	0	1	96	287

settings of operating system			(00.26)	(25.00)	(74.74)

Figures in bracket indicates Percentage

Further, it is seen that most of the users that is 58.33 percent, Change the security settings of browser occasionally followed by weekly is 23.18 percent yearly, 11.46 percent doing it monthly whereas 7.03 percent is weekly and no one is doing it on daily basis. Ratio of Change the security of browser setting also done occasionally is higher than that of daily, weekly, monthly and yearly.

Also 74.74 percent users change the security setting of operating system occasionally followed by 25 percent users doing it yearly and a very few that is 0.26 percent doing it monthly. Whereas no one is doing the setting of operating system on daily and weekly basis. So ratio of change the setting of operating system is occasionally is higher as compared to the weekly and yearly.

4.7 Comparative study of prevention and protection measures of various antivirus tools

An attempt was made to meet the fourth objective of the study and which is **"To do comparative study of prevention and protection measures of various antivirus tools."** The primary data collected from users has fulfilled this objective. Such an analysis also aims to know the comparison of prevention and protection techniques management of antivirus tools for personal computer in Pune City.

The internet is not a secure place by any means, and even the most tech-savvy users have a relatively high likelihood of downloading some form of malware or becoming the victim of an identity-stealing scam just by going online occasionally. There are many types of viruses that each has the ability to compromise PCs in different ways. Most typically, users acquire a virus by downloading questionable files that are falsely presented as other things in an email scam, or by visiting a phishing website. Once viruses have infected your computer, they can drastically slow down your processing speeds, delete critical and important personal files and images, and in the worst case, cause irreparable physical damage to your computer. Viruses can cost you thousands in computer-replacement costs and cause you to lose very important documents and photos.

4.7.1 Important parameters of Antivirus Software

An attempt is made to measure the importance of antivirus on the basis of various parameter, some observations have been laid down to be ranked on a 1 to 5 point Likert scale where, being 1 and 2 lowest responses while 4 and 5 represents highest. Point 3 represents moderation between the two extremes. From the responses, average value is calculated with regard to each observation. These observations are then ranked on the basis of average value. Here, the average value indicates that rank of parameters of importance of antivirus by users.

Table No. 4.29 shows the various parameters of importance of antivirus tools to understand quality parameters and capability of the present Antivirus Tool. To meet the objective question is designed by using various parameters which defines the importance of antivirus tools. It is observed that for each parameter average scale is in-between 1 to 5 that is in-between Excellent to poor. In fact all are above 3.5 which mean that with respect to all the parameters much improvement is observed.

It is observed that average value for Security is 4.78 followed by Malware detection is 4.55, followed by Firewall Security is 4.52, 4.34 is for Ease of use and 4.25 is for update frequency.

Further average value of database size is 4.15 followed by for safe banking is 4.11, for activity reporting is 4.10, for effect on system speed is 4.08 and also 4.01 for scanning speed, 4.00 is for startup protection. Further average value of Cost is 3.98 followed by registry is 3.93 whereas P2P/File sharing protection is 3.92, overall size in bytes is 3.90, Licensed arrangements is 3.89, web-page scanning/anti-phishing is 3.82 and free additional software is 3.4.

Table No.4.29: Antivirus Tool Important Parameters

Parameters	Most Imp	Imp	Neutral	Not Imp	Not at all Imp	Total	Avg. Value	Rank
Security	311 (80.99)	62 (16.15)	9 (02.34)	2 (02.52)	0 (00.00)	**384**	4.78	1
Malware detection	250 (65.10)	99 (25.78)	33 (08.59)	2 (02.52)	0 (00.00)	**384**	4.55	2

Firewall security	237 (61.72)	110 (28.65)	35 (09.11)	2 (02.52)	0 (00.00)	**384**	4.52	3
Ease of use	206 (53.65)	116 (30.21)	47 (12.34)	15 (03.91)	0 (00.00)	**384**	4.34	4
Update frequency	163 (42.45)	172 (44.79)	32 (12.24)	17 (04.43)	0 (00.00)	**384**	4.25	5
Database size	154 (40.10)	162 (42.19)	40 (10.42)	28 (07.29)	0 (00.00)	**384**	4.15	6
Safe Banking	160 (41.67)	120 (31.25)	90 (23.44)	14 (03.65)	0 (00.00)	**384**	4.11	7
Activity Reporting	159 (41.41)	120 (31.25)	90 (23.44)	15 (03.91)	0 (00.00)	**384**	4.10	8
Effect on System Speed	171 (44.53)	101 (26.30)	84 (21.88)	28 (07.29)	0 (00.00)	**384**	4.08	9
Scanning speed	144 (37.50)	123 (30.03)	92 (23.96)	25 (06.51)	0 (00.00)	**384**	4.01	10
start-up protection	125 (32.55)	170 (44.27)	52 (13.54)	37 (09.64)	0 (00.00)	**384**	4.00	11
Cost	129 (33.59)	144 (37.50)	85 (22.14)	26 (06.77)	0 (00.00)	**384**	3.98	12
Registry	120 (31.25)	158 (41.15)	67 (17.45)	39 (10.16)	0 (00.00)	**384**	3.93	13
P2P/File Sharing Protection	161 (41.93)	92 (23.96)	70 (18.23)	61 (15.89)	0 (00.00)	**384**	3.92	14
Overall size in bytes	115 (29.95)	137 (35.68)	109 (28.39)	23 (05.99)	0 (00.00)	**384**	3.9	15
Licensed Arrangements	126 (32.81)	140 (36.46)	68 (17.71)	50 (13.02)	0 (00.00)	**384**	3.89	16
Web-page scanning/	96 (25.00)	153 (39.84)	103 (26.82)	32 (08.33)	0 (00.00)	**384**	3.82	17

anti-phishing								
Free additional software	79 (20.57)	92 (23.96)	115 (29.95)	98 (25.52)	0 (00.00)	**384**	3.4	18

Figures in bracket indicates Percentage

Note: Average Scale 1 to 5 (where Most Important =5;Important =4; Neutral=3;Not Important=2 & Not at all Important=1)

All this indicates that the users are using antivirus tools to prevent and protect from virus. Antivirus software is an effective remedy that does not only cleans out the virus from your system but it also protects the system against virus attacks. If you have an antivirus program installed in your system, you will be able to create a strong protection for your computer system against the viral problems. The best thing about these antivirus programs is that they are easily downloadable and can be installed in your system without any charge.

Table No.4.30: Percentage wise Important parameters of AV Tools

Parameters	Most Important	Important	Per	Avg. Value	Rank
Security	311 (80.99)	62 (16.15)	373 (97.14)	4.78	1
Malware detection	250 (65.10)	99 (25.78)	349 (90.88)	4.55	2
Firewall security	237 (61.72)	110 (28.65)	347 (90.37)	4.52	3
Ease of use	206 (53.65)	116 (30.21)	322 (83.86)	4.34	4
Update frequency	163 (42.45)	172 (44.79)	335 (87.24)	4.25	5
Database size	154 (40.10)	162 (42.19)	316 (82.29)	4.15	6
Safe Banking	160 (41.67)	120 (31.25)	280 (72.92)	4.11	7

Activity Reporting	159 (41.41)	120 (31.25)	279 (72.66)	4.10	8
Effect on System Speed	171 (44.53)	101 (26.30)	272 (70.83)	4.08	9
Scanning speed	144 (37.50)	123 (30.03)	267 (69.53)	4.01	10
start-up protection	125 (32.55)	170 (44.27)	295 (76.82)	4.00	11
Cost	129 (33.59)	144 (37.50)	273 (71.09)	3.98	12
Registry	120 (31.25)	158 (41.15)	278 (72.40)	3.93	13
P2P/File Sharing Protection	161 (41.93)	92 (23.96)	253 (65.89)	3.92	14
Overall size in bytes	115 (29.95)	137 (35.68)	252 (65.63)	3.9	15
Licensed Arrangements	126 (32.81)	140 (36.46)	266 (69.27)	3.89	16
Web-page scanning/ anti-phishing	96 (25.00)	153 (39.84)	249 (64.84)	3.82	17
Free additional software	79 (20.57)	92 (23.96)	171 (29.95)	3.4	18

Table No. 4.30 also shows the rank of each parameter representing importance of antivirus tools. According to the above table, users believe that they are getting enough protection & prevention from antivirus tool but they still are giving

importance to 'Security' parameter as they have ranked it First weightage of 97.14 percent .It is followed by Second rank for Malware Detection with Weightage of 90.88 percent, Third rank is for Firewall security with weightage of 90.37 percent, fourth rank is for Ease of use with weightage of 83.86 percent. Also fifth rank is for Update frequency with weightage of 87.24 percent, sixth rank is for database size with weightage of 82.29 whereas seventh rank is for safe banking with weightage of 72.92, eighth rank is for activity reporting with weightage of 72.66 followed by nineth rank is for Effect of System Speed with weightage of 70.83 and tenth rank is for Scanning speed.

Further it is seen that eleventh rank is for startup protection with weightage of 76.82 percent followed by twelveth rank is for cost with weightage of 71.09, thirteenth rank is for Registry with weightage of 72.40 percent, fourteenth rank is for P2P/File Sharing Protection with weightage of 65.89 whereas fifteenth rank is for Overall size in byes parameter with weightage of 65.89 percent, sixteenth rank is for Licensed Agreements with weightage of 69.27, seventeenth rank is for Web-page Scanning/Anti-Phishing with weightage of 64.84 percent and further last means eigteenth rank is for free additional software with weightage of 44.53 percent.As per the responses, it is clear that users are satisfied with antivirus tools keep safely for performing day to day to activities.

4.7.2 Measurement of Satisfaction about the Antivirus tools

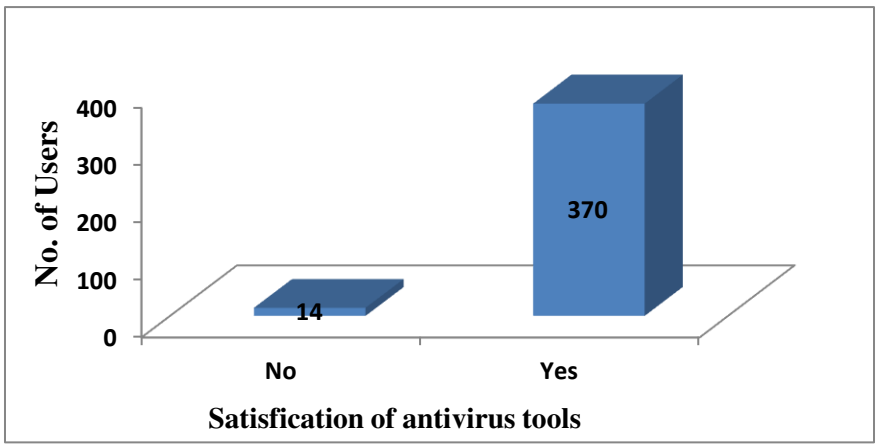
Research is mainly focused on management of antivirus tools used by the various types of the user for their personal computer. So there is need to measure the satisfaction level of antivirus tools among the users. Table No. 4.31 shows the users satisfaction with respect to antivirus tools used by user for their personal computers. It is observed that 96 percent users are satisfied antivirus tools whereas remaining 4 percent users are dissatisfied. According to these ratios, it shows that users are aware about the security of personal computer so that they are highly satisfied with antivirus tools.

Table No.4.31: User Satisfaction with respect to Antivirus Tool

User Satisfaction with antivirus tool	No. of Users
No	14(04.00)
Yes	370(96.00)
Total	384(100)

Figures in bracket indicates Percentage

Graph 4.19: User Satisfaction with respect to Antivirus Tool



Graph 4.19 shows the User Satisfaction with respect to Antivirus Tool used for their personal computers. Ratio of satisfaction among the user is very high as compared to the dissatisfaction. It can be concluded that the users are satisfactory with antivirus tools.

4.7.3 Measurement of User wise Satisfaction with the Antivirus tools

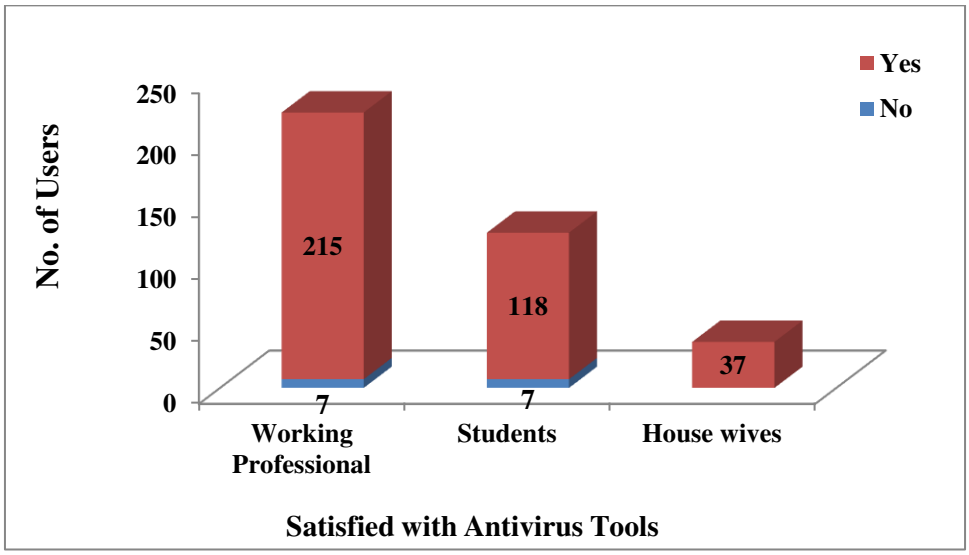
As a need of, measure the satisfaction level of various types of the user like working professionals, students and house wives. Table No. 4.32 shows the user wise satisfaction with antivirus tool. It is seen that 96.35 percent users are satisfies out of which 55.99 percent working professionals are satisfied with antivirus tools followed by 30.73 percent Student users are satisfied and 9.64 percent housewives are satisfies with antivirus tools. Only 3.65 users are not satisfied in which 1.82 percent working professionals and students. It is shows that all users are very much satisfied with all features of antivirus tools.

Table No.4.32: User wise Satisfaction of Antivirus Tool

User Type	No. of Users		Total
	Yes	No	
Working Professional	215(55.99)	7(01.82)	222(57.81)
Students	118(30.73)	7(01.82)	125(32.55)
House wives	37(09.64)	0(00.00)	37(09.64)
Total	370(96.35)	14(03.65)	384(100)

Figures in bracket indicates Percentage

Graph 4.20: Distribution of Respondents for user wise satisfied with antivirus tools



Graph No. 4.20 shows the user wise satisfied with antivirus tools. Ratio of satisfaction of users is very high as compared to the non satisfaction of users.

4.7.4. Antivirus wise user's satisfaction

For study purpose various antivirus tools of 6 companies are used so need to identify antivirus tool wise user satisfaction. Table No.4.33 shows distribution of antivirus tool wise user satisfaction. It is shows the antivirus wise user's satisfaction and their ranks according to users point of view It shows that out of 384 respondents, 57.81 percent users are satisfied with quick heal antivirus because it is supported various important

features such as parental control, antimalware,USB drive protection, database security has proved that Quick heal is most popular antivirus . From primary data it is clear that 49.22 percent users are satisfied with Net protector antivirus, its cost is very less as compared to other antivirus and it also support important features. It is followed by 18.75 percent users are satisfied with McAfee Virus. A very low satisfaction ratio for next antivirus is 18.49 percent for Kaspersky antivirus. Still 13.02 percent users are satisfied with Norton antivirus and lastly 12.24 percent are satisfied with AVG antivirus.

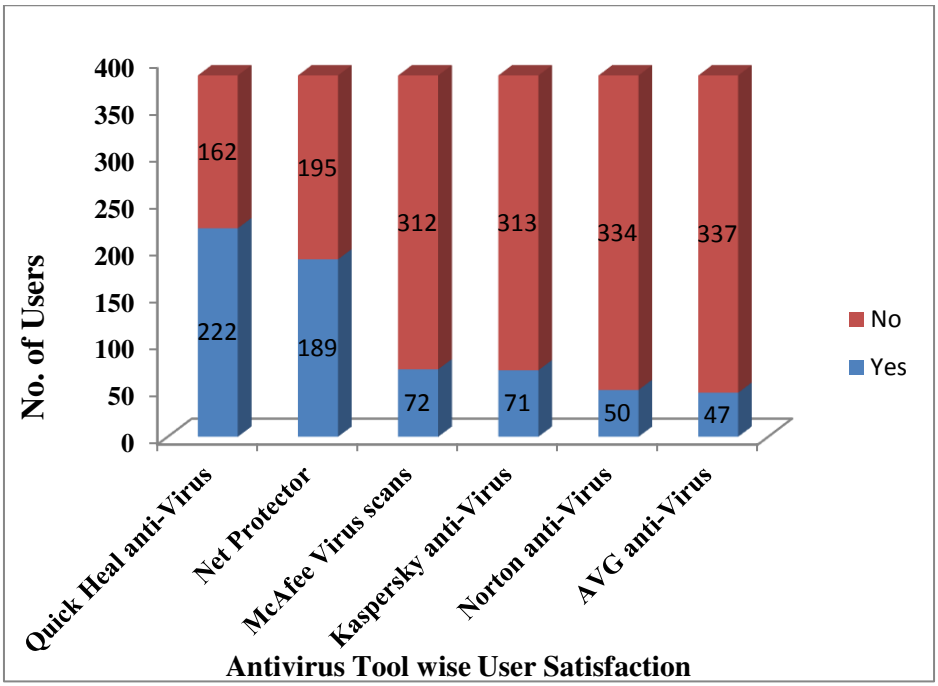
For satisfaction of antivirus working among users, users prefer to rank the satisfaction ratio about antivirus. According to antivirus wise ranking first rank goes to Quick Heal followed by second to Net protector, third is McAfee virus, fourth is for Kaspersky, fifth is Norton, and last one means six is AVG..

Table No.4.33: Antivirus Tool wise User Satisfaction

Antivirus Tool	Quick Heal anti-Virus	Net Protector	McAfee Virus scans	Kaspersky anti-Virus	Norton anti-Virus	AVG anti-Virus
Yes	222 (57.81)	189 (49.22)	72 (18.75)	71 (18.49)	50 (13.02)	47 (12.24)
No	162 (42.19)	195 (50.78)	312 (81.25)	313 (81.51)	334 (86.98)	337 (87.76)
Rank	1	2	3	4	5	6

Figures in bracket indicates Percentage

Graph 4.21: Antivirus Tool wise User Satisfaction



Graph No. 4.21 shows the antivirus wise satisfaction ratio 57.81 percent users prefer to use quick heal followed by 49.22 is users are satisfied with net protector and 18.75 percent users satisfied with McAfee antivirus. Further 18.49 percent users prefers Kaspersky antivirus for security purpose, 13.02 Percent citizens prefer Norton antivirus and 12.24 percent users are prefer AVG.

Here all 384 users have given their opinion about all antivirus companies' products because they might have used the antivirus tool at work place or on home pc. Most of the users change antivirus tools frequently as per their requirement, liking, usage and budget.

It is seen that 57.81 percent users are prefer to use Quick heal antivirus for protection against virus as compared to other antivirus. Hence this data supports the proving the objective of the study that satisfaction of users antivirus wise.

Presentation and Analysis of Data related to Vendors of Antivirus tools

4.8 Services provided by antivirus provider companies and its impact on various users.

Computer viruses have been around almost as long as computers. Computer viruses have dramatically increased in complexity over the years. Antivirus tool is evaluated using parameters like cost, service and performance. This showed that people were aware about the problems caused by viruses and also the importance of antivirus. The viruses have a big impact to the users especially when they were unable to perform their daily routine work due to viruses.

4.8.1 Services provided by antivirus provider companies and its impact on various users.

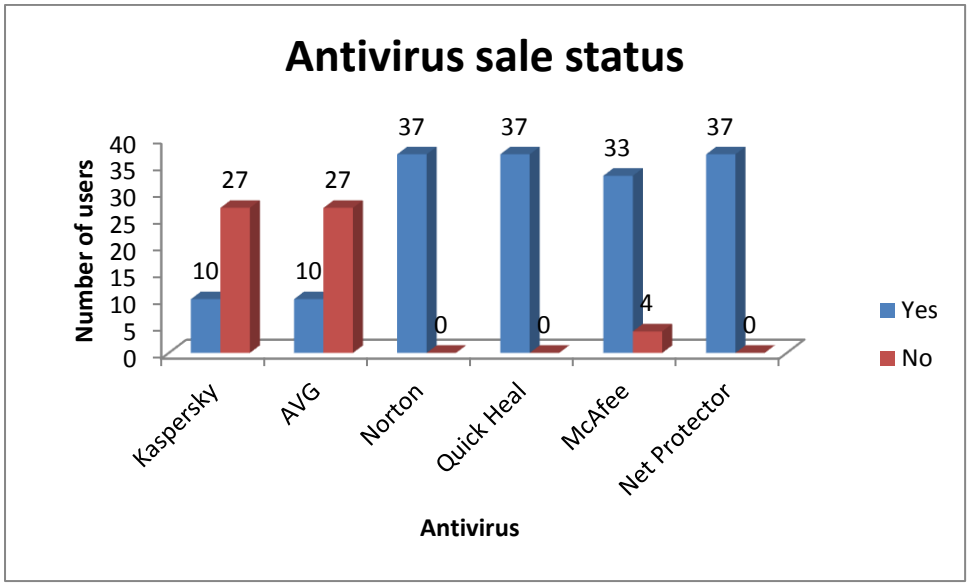
From table No.4.34 shows the distribution of the respondents according to their responses for about antivirus tool mostly sold by various antivirus companies. It is seen that most of the antivirus tools Quick Heal, Norton &Net Protector are sold Mostly .It is followed by McAfee sold by 89 percent further , Kaspersky & AVG sold by 27 percent. So Maximum sale of Ant viruses are Norton,,Quick Heal & Net protector.

Table No. 4.34: Antivirus Tool Sales Status

Antivirus Tool Sales Status	Yes	No
Kaspersky	10(27)	27(73)
AVG	10(27)	27(73)
Norton	37(100)	0(0)
Quick Heal	37(100)	0(0)
McAfee	33(89)	4(11)
Net Protector	37(100)	0(0)

Figures in bracket indicates percentage

Graph 4.22: Antivirus tool sold Mostly



Above Graph 4.22 shows that maximum sale of antivirus are Norton, Net Protector & Quick Heal followed by McAfee and further sale of antivirus are Kaspersky & AVG.

4.8.3 Popular type of Antivirus product

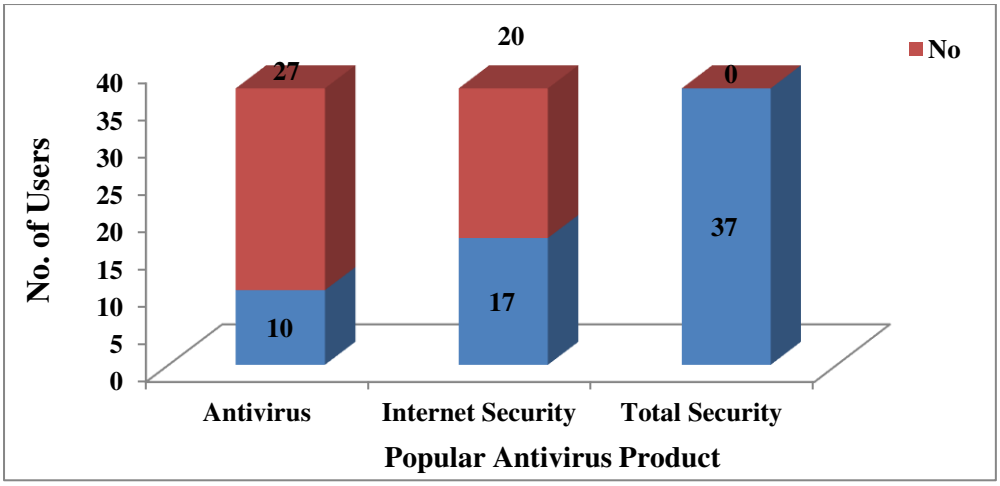
From table no. 4.35, shows the distribution of the respondents according to the type of product purchased by them. It is seen that most of the user are using Total security product (100 percent) .It is followed by Internet security product is 46 percent. Further, antivirus product is 10 percent. It is seen that, popular product is total security.

Table No.4.35: Popular type of Antivirus product

Type of Antivirus product popular	Yes	No
Antivirus	10(27)	27(73)
Internet Security	17(46)	20(54)
Total Security	37(100)	0(0)

Figures in bracket indicates Percentage

Graph 4.23: Popularity of Antivirus product



Above Graph 4.23 shows that popular antivirus product is total security followed by internet security and further antivirus product. So it is seen that maximum usages of popular product is total security.

4.8.4. Purchase pattern of Antivirus by user

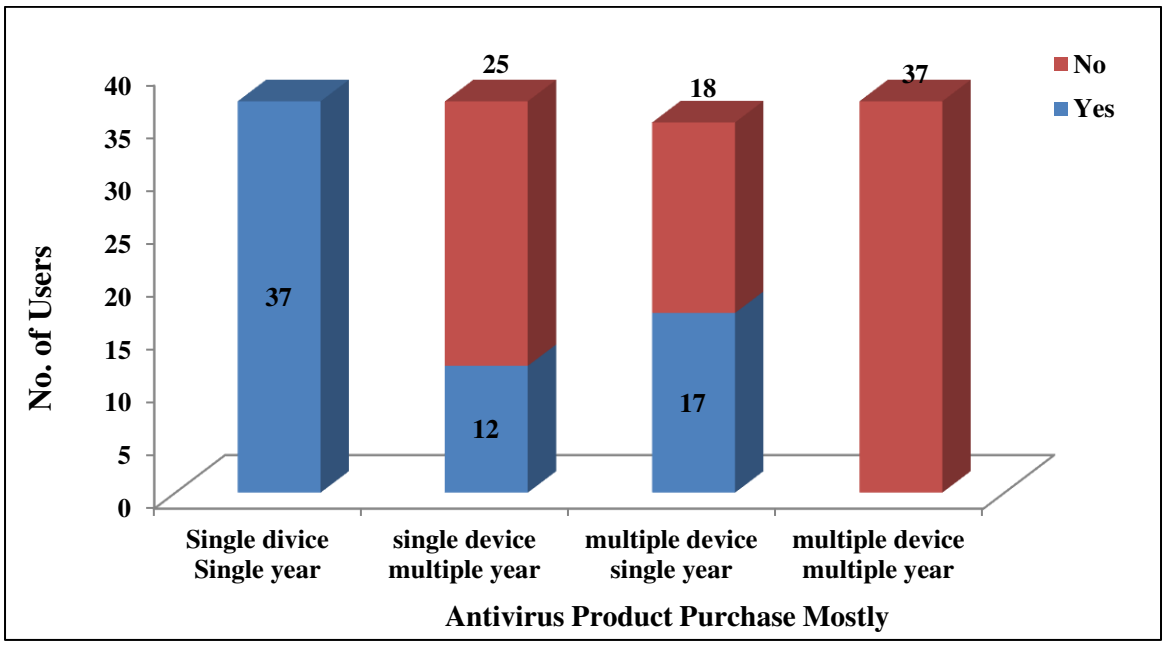
From table no .4.36, shows the distribution of the respondents according to their responses for about Purchase pattern of Antivirus by user by various antivirus companies. It is seen that most of the user are purchased single device for single year is 100 percent. Further, single device for multiple years 32 percent.

Table No.4.36: Antivirus products are purchased Mostly

Antivirus products are purchased Mostly	Yes	No
Single device Single year	37(100)	0(0)
single device multiple year	12(32)	25(68)
multiple device single year	17(46)	18(49)
multiple device multiple year	0(0)	37(100)

Figures in bracket indicates Percentage

Graph 4.24: Antivirus products are purchased Mostly



Above Graph 4.24 shows most popular product are purchased by users. It is seen that Single device for single year is purchased mostly by users. It is followed by multiple device for single year and further single device for multiple year are purchased. So it is seen that maximum users are purchased single device for single year.

4.8.4 Cost of Antivirus Tools

From table no.4.37 shows the distribution of antivirus tools versus cost factor for single and multiple device for 1and more than 1 year according to their responses of vendors.

Table No.4.37: Cost of antivirus Tools

Cost Factor	Antivirus Tool	Less than Rs. 500	Rs. 501 to 1000	Rs. 1001 to 1500	Rs.1501 to 2000	More than Rs. 2000
cost of antivirus supporting Single Device	Kaspersky	0	37 (100)	0	0	0
	Norton Security	0	37	0	0	0

Annually			**(100)**			
	AVG anti-Virus	**0**	**37(100)**	**0**	**0**	**0**
	McAfee	**0**	**37(100)**	**0**	**0**	**0**
	Quick Heal	**0**	**37(100)**	**0**	**0**	**0**
cost of antivirus supporting Multiple Device Annually	Kaspersky	**0**	**37(100)**	**0**	**0**	**0**
	McAfee	**0**	**37(100)**	**0**	**0**	**0**
	Quick Heal	**0**	**37(100)**	**0**	**0**	**0**
cost of Internet security products supporting Single device & multiple years	Kaspersky Internet security 1 device 3 years	**0**	**0**	**37(100)**	**0**	**0**
	Quick Heal Internet security 1 user 3 years	**0**	0	**37(100)**	**0**	**0**
cost of Internet security products supporting Multiple device annually.	Kaspersky Internet security (3 pcs)	**0**	**0**	**0**	**0**	**37(100)**
	Norton security Deluxe (5 devices)	**0**	**0**	**0**	**37(100)**	**0**
	AVG Protection PRO (unlimited PCS)	**0**	**0**	**0**	**37(100)**	**0**
	McAfee Internet security1 year unlimited devices	**0**	**0**	**37(100)**	**0**	**0**

	Quick Internet security 3 users I year	**0**	**0**	**37(100)**	**0**	**0**
cost of Total security products supporting Multiple device annually	Kaspersky Total Security 3 PCS	**0**	**0**	**0**	**0**	**37(100)**
	Norton Security Premium (10 devices)	**0**	**0**	**0**	**0**	**37(100)**
	AVG Ultimate (Unlimited Installations)	**0**	**0**	**0**	**0**	**37(100)**
	McAfee Total Protection 1 year unlimited devices	**0**	**0**	**0**	**37(100)**	**0**
	Quick Heal Total Security 3 users 1 year	**0**	**0**	**0**	**0**	**37(100)**
	Net Protector Total Security 3 PCS	**0**	**0**	**0**	**0**	**37(100)**

Figures in bracket indicates Percentage

Above table shows that, Kaspersky, AVG, Nortn, QuickHeal &McAfee antivirus tools having price between Rs.501 to Rs.1000 and it supporting Single Device Annually. KasperSky, AVG antivirus tools having cost between Rs.501 to Rs.1000 and Quick Heal having cost is Rs.1001 to Rs.1500 and it supporting Multiple Device Annually. Kaspersky Internet security 1 device 3 years having cost is Rs.1001 to Rs.1500 and Quick Heal Internet security 1 user 3 years cost is more than Rs.2000 and theses Internet security tools are supporting for Single device & multiple years. Kaspersky Internet security (3 pcs) and Norton security Deluxe (5 devices) having cost is Rs.1501 to Rs.2000, AVG Protection PRO (unlimited PCS), McAfee Internet security1 year unlimited devices having cost is Rs.1001 to Rs.1500 and Quick

Internet security 3 users 1I year having cost is more than Rs.2000 and supporting Multiple device annually. The Total security products are like Kaspersky Total Security 3 PCS, Norton Security Premium (10 devices), McAfee Total Protection 1 year unlimited devices, & Quick Heal Total Security 3 users 1 year having cost is more than Rs.2000 and AVG Ultimate (Unlimited Installations) having cost is Rs.1501 to Rs.2000 where as Net Protector Total Security 3 PCS having cost is Rs.501 to Rs.1000.

4.8.5. Popularity Reason of Antivirus Tools

An attempt was made to meet the fifth objective of the study and which is "To study the reason behind the popularity of antivirus tool." The primary data collected from vendors has fulfilled this objective. Some observations have been laid down to be ranked on a 1 To 5 point Likert scale where, being 1 and 2 lowest responses while 4 and 5 represents highest. Point 3 represents moderation between the two extremes. From the responses, average value is calculated with regard to each observation. Here, the average value indicates that rank of Popularity Reason of various antivirus tools by vendors.

In a 5-point Likert Scale, having categories like Strongly Agree,Agree , Neutral, disagree & Strongly disagree are clubbed into three categories. Hence, this five category scale has been collapsed into three categories one like favourable, neutral and unfavourable perception. The reason for having mixture of favorable, neutral and unfavorable statements in a Likert scale is the responses by the respondents should not become monotonous while answering the questions. Hence, researcher has also applied 5-point Likert Scale and calculates weighted average value.

To meet the objective, questions were designed using various parameters which defined the Reasons for popularity of antivirus tools. It was observed that for each parameter average scale is calculated between 1 to 5 i.e. from Strongly disagree to Strongly Agree.

Table No.4.38: Popularity Reason of Antivirus Tools

Antivirus Tool	Popularity Reason of Antivirus Tools	Strongly disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Avg Value
Kasper Sky	Low cost	21 (56.75)	15 (40.54)	1 (2.70)	0 (00.00)	0 (00.00)	1.46
	Best Performance	0(00.00)	0 (00.00)	0 (00.00)	15 (40.54)	22 (49.46)	4.59
	Best Service	0 (00.00)	0 (00.00)	0 (00.00)	15 (40.50)	22 (49.46)	4.59
Norton	Low cost	21 (56.75)	15 (40.54)	1 (2.70)	4 (10.81)	4 (10.81)	1.46
	Best Performance	0 (00.00)	0 (00.00)	0 (00.00)	15 (40.54)	22c	4.59
	Best Service	0 (00.00)	0 (00.00)	4 (10.81)	15 (40.54)	22 (40.54)	4.59
AVG	Low cost	21 (56.75)	15 (40.54)	1 (2.70)	4 (10.81)	4 (10.81)	1.46
	Best Performance	0 (00.00)	0 (00.00)	0 (00.00)	15 (40.54)	22 (40.54)	4.59
	Best Service	0(00.00)	0(00.00)	4 (10.81)	18	15	4.3
McAfee	Low cost	22 (49.46)	15 (40.54)	4 (10.81)	4 (10.81)	4 (10.81)	1.41
	Best Performance	0 (00.00)	9 (24.32)	0 (00.00)	28	0 (00.00)	3.51
	Best Service	0 (00.00)	0 (00.00)	4 (10.81)	18 (48.65)	15 (40.54)	4.3
Quick Heal	Low cost	22 (49.46)	13 (35.13)	2 (5.43)	0 (00.00)	0 (00.00)	1.46
	Best Performance	0 (00.00)	0 (00.00)	0 (00.00)	6 (16.22)	31 (83.78)	4.84
	Best Service	0 (00.00)	0 (00.00)	0 (00.00)	6 (16.22)	31 (83.78)	4.84
Net protector	Low cost	0 (00.00)	0 (00.00)	0 (00.00)	0 (00.00)	37 (100.00)	5
	Best Performance	2 (05.41)	1 (02.70)	1 (2.70)	24 (64.86)	9 (24.32)	4
	Best Service	1 (02.70)	2 (05.41)	2 (05.41)	13 (35.14)	19 (51.35)	4.27

Figures in bracket indicates Percentage

Note: Average Scale 1 to 5 (where Strongly Agree=5; Agree=4; Neutral=3; Disagree=2 & Strongly Disagree=1)

It is seen that highest scale for Kasper Sky are for Best Performance and Services (4.59).and Low cost (1.46) .It is followed by Norton antivirus tools highest scale for Best Performance and Services (4.59) and Low cost (1.46). AVG antivirus tools highest scale for Best Performance (**4.59),** Services (4.30) and Low cost (1.46). McAfee antivirus tools highest scale for Best Service (**4.3),** Best Performance (3.51) and Low cost (1.41). Quick Heal antivirus tools highest scale for Best Performance and Services (4.84) and Low cost (1.46).It is followed by Net protector highest scale for Low cost (5),Best Service (4.27) and Best Performance (4.00) .

Therefore, it can be inferred that the Low cost is for **Net protector** and Best performance and Best services are provided by **Quick Heal** antivirus tool. Majority of the users are satisfied with this service provided by their Anti-virus tool provider.

4.8.4 Services after purchasing as per Antivirus company‘s Point of View

Antivirus company providing various kind of services to users after purchasing such as Telephonic support, Onsite support, Remote Support & E-mail Support.
From Table No.5.36 shows services provided by Antivirus Company to user after purchasing the antivirus.

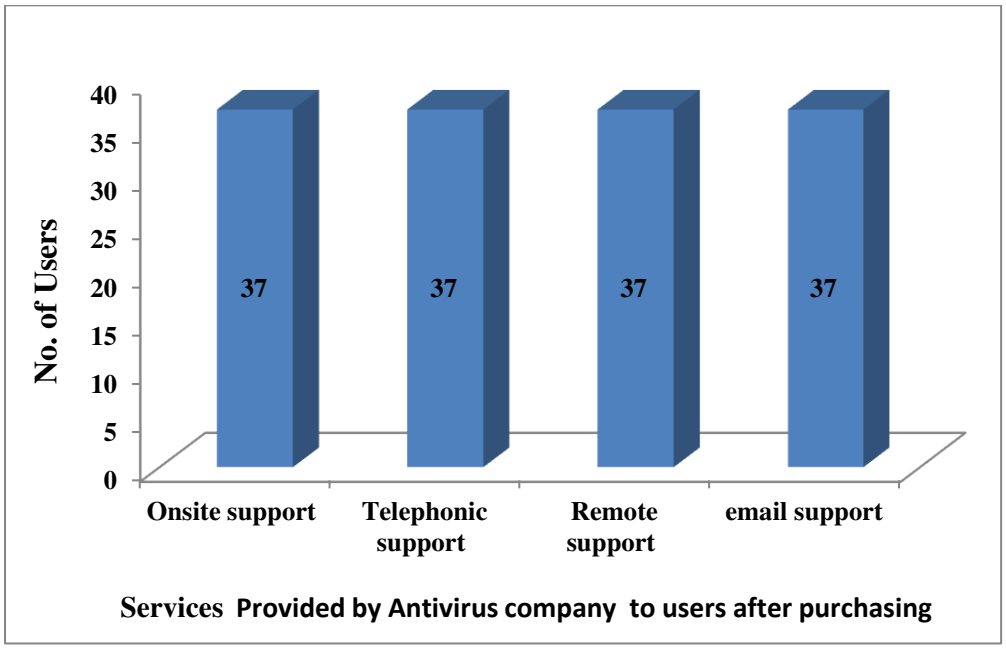
Table No.4.39: Services after purchasing as per Antivirus company‘s Point of View

Services Antivirus company provide to users after purchasing the antivirus tool	Yes	No
Onsite support	**37(100)**	**0(00.00)**
Telephonic support	**37(100)**	**0(00.00)**
Remote support	**37(100)**	**0(00.00)**
Email support	**37(100)**	**0(00.00)**

Figures in bracket indicates Percentage

It is seen that, all services are provided by Antivirus Company (100 percent) to users after purchasing antivirus tool.

Graph 4.25: Services after purchasing as per Antivirus company's Point of View



Above Graph 4.25 shows different services are provided by Antivirus Company to users. It is seen that Vendors are providing full support to antivirus users.

4.8.4 Services after purchasing as per User's Point of View

Antivirus company providing various kind of services to users after purchasing such as Telephonic support,Onsite support,Remote Support & E-mail Support.

From the above table No. 4.37 users perception about the various services are provided by the Antivirus Company. it is clear that 99 percent user are satisfied with the Online Support and Telephonic support. It is followed by 96 percent user satisfied with Email Support and 90 percent users are satisfied with remote service.

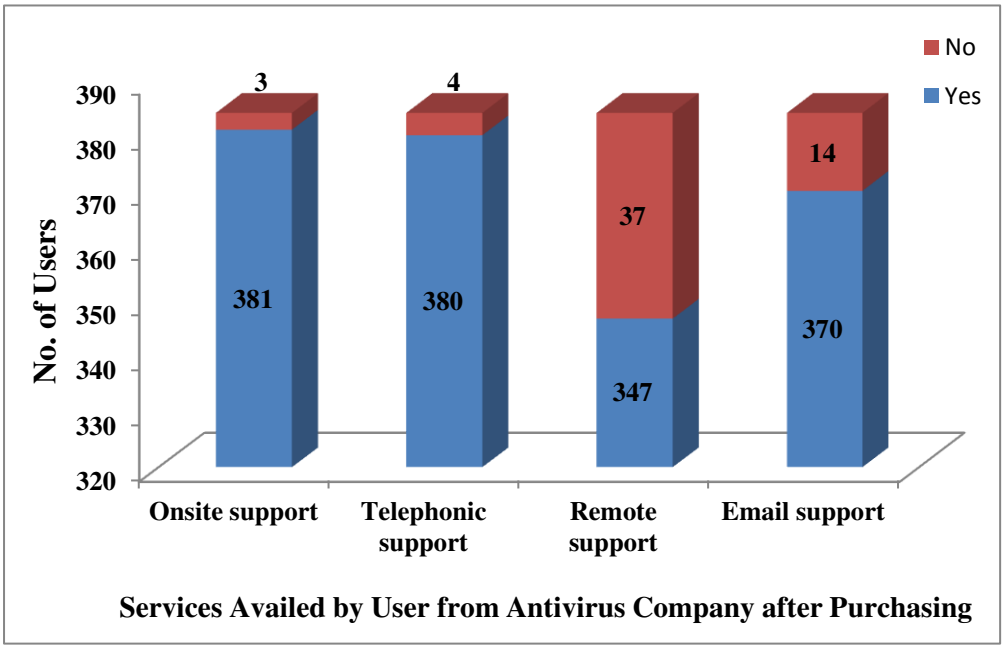
Table No.4.40: Services Availed by User from Antivirus Company after Purchasing

Support After Purchasing	Yes	No
Onsite support	381(99)	3(1)
Telephonic support	380(99)	4(1)
Remote support	347(90)	37(10)
Email support	370(96)	14(4)

Figures in bracket indicates Percentage

From Graph No.4.26 shows that users perception about various services by Antivirus Company.

Graph 4.26: Services Availed by User from Antivirus Company after Purchasing



Therefore, it can be inferred that the Online Support service provided by all the brands is above the expectations of the users. Since most of the times the users when in need of solution to their problems related to viral infection or installation process of the Anti-virus software, take the option of telephonic support service provided however most of the times this service is available. It is seen that the Email support facility of all the brands give complete protection from viruses that may enter the

system through promotional mails received. Thus this service is good to the different category of users.

Testing of Hypotheses

4.9 Testing of Hypotheses

The method of testing the hypotheses is described in Para 3.6 earlier. As explained there, many of the statistical tools used for generalization cannot be used in this study to test the hypotheses. If the replies of a majority of the respondents support a hypothesis that hypothesis will be considered as confirmed. Otherwise it will be considered as rejected. The data connected with the hypothesis, obtained from respondents is mostly used for this purpose. Conclusions of earlier studies made elsewhere may also be used supplement to the hypotheses of the study.

The following hypotheses have been tested based on the available data:

1. As a security reason, personal computer users are highly used licensed edition of antivirus tools.
2. Managing antivirus tool is at the most necessary for safe use of personal computer
3. While Purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand

Hypothesis 1

The first hypothesis of the study is "As a security reason, users are highly using licensed edition of antivirus tools."

H0 Null Hypothesis: 92 % or more user have positive attitude towards uses of antivirus tool.(H0: p = 0.92)

H1 Alternate Hypothesis: <92% user have positive attitude towards uses of antivirus tools. (H1= p < 0 .92)

This hypothesis is tested by using the usage of licensed and free version of antivirus tools used by the user by using percentage. It is seen that majority of the users (92.19 percent) are using licensed version of antivirus tool. (**Ref: Table No.4.10: Edition of Antivirus Tools**).

Table No.4.10: Edition of Antivirus Tools

Version of antivirus tools	No. of Users
Licensed	354(92.20)
Trial	16(04.20)
Both	14(03.60)
Total	384(100.00)

Figures in bracket indicates Percentage

Table No. 4.41 Z – Statistics of Edition of Antivirus Tool

Respondents	Sample size	Proportion	Standard error	z - statistic	p Value
Users	384	0.9220	1.384438	0.144462	0.442592

As the sample size = 384 (> 30) so in this case Z-test and as one proportion is involved. As alternative hypothesis is in terms "if less than" hence rejection area is towards only one side hence it is one tail test at 5 Percent level of significance is considered. Table value for one tail test is 1.64. The decision rule is that if the calculated value of z is greater than 1.64, and then rejects the null hypothesis and if z is less than 1.64, do not reject the null hypothesis, accept it.

Calculation of S.E. (Standard Error)

$S.E=\sqrt{pq/n}$ Where $p = 92$

$q = 100-92 = 8$

$n = 384$

$S.E. = \sqrt{92 * 8/ 384} =$ **1.384438**

Standard Error (S.E.) for percentage = **1.384438**

Step IV: Calculation of Z value

Z= diff. / S.E. diff = 92.20 – 92= 0.20

Z = 0.144462

As Z_{Cal}= |Diff| /S.E. is less than 1.64

Z statistics of licensed antivirus Tool is 0.144462 < 1.64 and also the p value (0.442592) > 0.05, there is no enough evidence to reject the null hypothesis. Hence accept Null hypothesis at 5 Percent level of significance. Thus it is seen that 92 percent users have positive attitude towards licensed edition of antivirus tool means "As a security reason, personal computer users are highly using licensed edition of antivirus tools" and hence the hypothesis **is accepted.**

4.13.2 Hypothesis 2

Second hypothesis of the study is "Managing antivirus tool is utmost necessary for safe use of personal computer"

This hypotheses is based on responses gathered from the users about the Managing antivirus tool is at the most necessary for safe use of personal computer. The responses collected from the user by using structured questionnaire. Details of responses were taken using 3 point scales like Satisfactory – 3; Can't Say– 2 and Not Satisfactory –1.

Table No.4.27: Settings of present Antivirus Tool by the User

Types of Setting	Satisfactory	Can't Say	Not Satisfactory	Average Value
On Scan Scheduling	328(85.42)	47(12.24)	9(02.34)	2.83
Internet and network	320(83.33)	64(16.67)	0(00.00)	2.83
External drives and devices	320(83.33)	64(16.67)	0(00.00)	2.83
Emails	302(78.65)	64(16.67)	18(04.69)	2.74
Password Protect Settings	296(77.21)	66(17.19)	21(05.60)	2.71
Files and folders	288(75.00)	77(20.05)	19(04.95)	2.70
Parental Control	200(52.08)	152(39.58)	32(02.34)	2.44

Figures in bracket indicates Percentage

As per Table No.4.27: Management of Antivirus Tool by the User, the percent and average scale of responses were calculated by using the ratings. It is clear that all Average values are greater than 2.70 hence it proves that respondents are more satisfied with settings. It is shows that settings are required for management of antivirus tools.

Also the calculated value of average point rating scale is greater than 2.70 which represents the majority of the users are agreed about the types of setting are required for managing the antivirus tools at the most necessary for safe use of personal computer. Therefore, it is to be concluded that, the hypotheses which is stated in the present study is **positively accepted.**

4.13.3 Hypothesis 3

Third Hypothesis of the study is "While Purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand"

H0 Null Hypothesis: 78 % or more user agreed that While Purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand.(H0: p = .78)
H1 Alternate Hypothesis: <78% user agreed that While Purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand.(H1= p < .78)

H0 : p =0.78

H1= p < 0.78(One tail test as rejection area is towards one side)

Step II: Sample Size

n=384 (> 30)

As n > 30, large sample test i.e. Z-test is used.

This hypothesis is tested by using the selection criteria of antivirus tools used by the user while purchasing of antivirus tool by using percentage. It is seen that majority of the users (78.90 percent) are applied brand as a selection criteria while purchasing antivirus tools. (**Ref: Table No. 4.9: Selection Criteria of Antivirus Tools**).

Table No.4.9: Selection Criteria of Antivirus Tools

Selection Criteria of antivirus tools	**No. of Users**
Brand	303(78.90)
Service	39(10.20)
Price	42(10.90)
Total	384(100.00)

Figures in bracket indicates Percentage

Step III: Calculation of S.E. (Standard Error)

$S.E=\sqrt{pq/n}$ Where p = 78
q = 100-78 = 22
n =384

S.E. = $\sqrt{78 * 22/ 384}$= **2.1187**

Step IV: Calculation of Z value

Z= diff. / S.E. diff = 78.90 - 78

Z_{cal}= 0.4247

Step V: Comparison:

Table value of Z for one tail test at 5% level of significance is 1.64

Table No. 4.41 Z – Statistics of Edition of Antivirus Tool

Respondents	Sample size	Proportion	Standard error	z - statistic	p value
Users	384	0.7890	2.1187	0.4247	0.335528

Step VI: Conclusion:

Z statistics of edition of antivirus tools is 0.4247 < 1.64 also the p value (0.335528) > 0.05, there is no evidence to reject null hypothesis. Hence accept Null hypothesis at 5 Percent level of significance. Thus it is seen that 78 percent users have positive attitude towards selection of brand of antivirus tools while purchasing it means "While Purchasing of antivirus tool, Selection of antivirus tool is closely associated with the Brand" and hence **the hypothesis is accepted.**

CHAPTER 5

FINDINGS, CONCLUSIONS AND SUGGESTIONS

5.1. Introduction

This chapter presents the findings of the study. Next the conclusions and suggestions arising out of the study are presented. It was observed during the course of the study that published research material on the subject of the study was strictly limited and a number of areas and aspects require wider and in-depth research in future. The scope for future research is therefore briefly discussed before concluding the chapter. For ready reference and convenience, referent table numbers of the study are given in brackets in the concerned paragraph of the chapter.

5.2 Findings

The findings set forth in the following pages constitute a recapitulation in a short form of what has been attempted at length in earlier chapters. This study mainly relates to the management of antivirus tool with respect to personal computer's user. It considers awareness and usage of antivirus tool among the users like working professionals, students and house wives with respect to their personal computers. It studies the products of antivirus companies like AVG, McAfee, Kaspersky, Norton, Net Protector and Quick Heal. It also considers various categories of antivirus tools such as Antivirus, Internet Security and Total Security and their prevention techniques to measure the security and avoidance of threats.

The study finds the problems faced by users while using antivirus tools including financial loss and number of other threats.

It also finds settings of antivirus tools and its impact on security and threats as per the user's point of view and also support provided by antivirus company during and after purchasing. All objectives focus on management of antivirus tool of user's of personal computer, antivirus tools awareness and impact of usage, impact of security settings and cost factor while purchasing antivirus tool and support from the vendor.

The researcher of this study has considered various types of the antivirus tool and its impact at national and international level. This unique approach has provided new insights, added to the important conclusions and enriched this study. The researcher has analyzed the primary data to study the management of antivirus tools with respect

to personal computers, problems with respect to usage and settings of antivirus tool and vendor support to keep antivirus tool up to date. Findings related to antivirus users is presented in Part I and findings related to antivirus vendors is presented in part II.

5.2.1 Part I: Findings related to Users of Antivirus Tools

1. It was seen that 31.51 percent working professionals are male as compared to the 26.30 percent are female respondents. So ratio of male working professionals is higher than that of female working professionals. Whereas 21.61 percent are male students and 10.94 percent are female students. So in student's category, ratio of male students is higher than that of female students. And 9.63 percent house wives contributed and their ratio is very low as compared to other user types. (Table No.4.4). Hence it is concluded that the ratio of male users is slightly higher as compared to female users.
2. It was seen that a majority of over 50.52 percent users are Post graduates. Out of which 25 percent are working professionals whereas 24.74 percent are students and only 2.34 percent are housewives followed by 33.85 percent users who have completed their graduate & above degree, out of which 24.74 percent are working professionals, 7.03 percent are students and 2.08 percent are housewives. A further 10.68 percent user has completed their higher secondary education, out of which 5.21 percent are working professionals, 2.34 percent are students and 3.3 percent are housewives. The rest of the 5.47 percent users have completed their education upto higher secondary, out of which 2.86 percent are working professionals and 3.13 percent are housewives. Up to 10^{th} students not considered for study purpose, as they are not enough mature and understand security concept and its effectiveness & efficiency. (Table No.4.5).The proportion of Post graduate user is higher to graduate & above user and the proportion of higher secondary & above educated user is higher than up to higher secondary educated users. (Table No.4.5).
3. It has been observed that most of the working professionals like 57.80 percent are contributed for study followed by 32.60 percent students and remaining 9.60 percent House wives. So ratio of working professionals is higher than that of students and house wives.(Table No.4.6).
4. It has been concluded that,100 percents users are aware about Antivirus tools.(Table No.4.7).

5. It was clear that, 57.81 percent working professionals are aware about antivirus tools followed by 32.55 percents students are aware about antivirus tools and 9.64 percents housewives aware about antivirus tools.(Table No. 4.8)
6. It was seen that 78.90 percent users preferred brand while purchasing antivirus tool followed by 10.90 percent users preferred price and further 10.20 percent users preferred service provided by the vendor(Table No. 4.9).
7. It was observed that, 92.20 percent user used licensed edition followed by 4.20 percent user used trial edition and 3.60 percent user used both versions.(Table No.4.10)
8. It was seen that maximum number of users that is 92.19 percent users used licensed edition of antivirus tools. Out of which 55.99 percents are working professionals followed by 26.82 percent are students and only 9.19 percent house wives used licensed edition of antivirus tools. Whereas 4.16 users used trial edition of antivirus tools out of which only 0.78 percent are working professionals and 2.60 percent are students and only 0.78 percent were house wives. Also it wss seen that only 3.65 percent users used both the editions. Out of which 1.04 percent are working professionals followed by 2.35 percent are students and only 0.26 percent are house wives.(Table No. 4.11)
9. It has depicted that out of 384 users, 58.33 percent user's used Quick Heal Antivirus tool for their personal computer. As a quick heal is strongest antivirus tools as compared to other antivirus tools. Followed by 50.26 percent user's used Net Protector antivirus tools, 20.05 percent used McAfee. Further 18.49 percent user's used Kaspersky , 14.06 percent user's used Norton antivirus tool and only 13.02 percent user's used AVG antivirus tools. Hence it is clear most of the users are in favor of Quick Heal antivirus tool in terms of security reason.(Table No. 4.12)
10. It was seen that 58.33 percent users used quick heal antivirus tool for security purpose. Out of which 37.50 percents are working professional followed by 20.83 percent students and further no one from housewives category uses quick heal. 50.26 percent users used Net Protector antivirus tool, out of which 31.25 percent are working professionals, 9.38 percent are students and 9.64 percent are housewives. Whereas 20.05 percent users used McAfee antivirus tool, out of which 13.28 percent are working professionals, 6.77 percent are students and again no one from house wives category. It has been observes that 18.49 percent

users used Kaspersky antivirus tool which includes 12.76 percent working professionals, 5.73 percent students and no one from house wives category. Also only 14.06 percent users used Norton antivirus tools, out of which 7.03 percent are working professionals followed by 3.13 percent are students and only 3.91 percent are house wives. Also 13.54 percent users uses AVG antivirus tool which includes 8.85 percent are working professionals and 4.69 percent are students.(Table No. 4.13)

11. It was found that 55.70 percent users prefer antivirus tool with cost less than Rs. 1000/- whereas 28.50 percent users purchased antivirus tool in range Rs. 1001/- to Rs. 1500/-. Only 8.30 percent users preferred antivirus tool in range from Rs. 1501/- to Rs. 2000/- further only a few like 1.80 percent users preferred antivirus tool in range Rs.2000/- to Rs. 2500/- and only 5.70 percent users were ready to pay cost more than Rs. 2500/-(Table No. 4.14).
    - It was seen that 55.70 percent users preferred to purchase antivirus with amount less that Rs. 1000/-, out of which 13.02 percent user preferred purchase of Quick Heal, 25 percent purchased Net Protector, 7.03 percent purchased McAfee, 3.65 percent purchased Kaspersky, 3.91 percent purchased Norton and only 3.13 purchased AVG. It is followed by 28.40 percent users purchased antivirus tools in between range of Cost of Rs. 1001/- to Rs. 1500/-, out of which 11.72 percent user preferred to purchase of Quick Heal, 7.29 percent bought Net Protector, 2.86 percent purchased McAfee, 2.34 percent purchased Kaspersky and a few 2.08 percent purchased Norton & AVG. (Table No. 4.15).
    - It was seen that, 8.30 percent users purchased antivirus tools in between range of Cost of Rs. 1501/- to Rs. 2000/-, out of which 3.13 percent user preferred purchase of Quick Heal, 1.30 percent purchased Net Protector & McAfee, 1.04 percent purchased Kaspersky & AVG and a few 0.52 percent purchase Norton . (Table No. 4.15)
    - It was also observed that only 1.82 percent users purchase Quick Heal and no one from other categories of antivirus tools from cost range in between Rs.2001/- to Rs. 2500/-. (Table No. 4.15).
    - Also 5.70 percent users purchased Antivirus tools with cost more than Rs. 2500/-, out of which 2.60 percent users bought Quick Heal, a few 0.52 percent users purchased Net Protector,1.30 percent users purchased

McAfee & Kaspersky and no one purchase Norton & AVG. (Table No. 4.15).

12. As per the primary data, it was observed that 78.64 percent users installed total security antivirus tool followed by 14.30 percent users used internet security antivirus tools and further only 7 percent users using home edition.(Table No.4.16)
    - It was observed that 58.07 percent working professionals installed antivirus tools on their personal computers out of which 43.75 percent users installed total security followed by 10.68 percent users installed internet security and 3.65 percent users installed home edition on their personal computers.
    - It was also observed that 32.29 percent students installed antivirus tool on their personal computer, out of which 25.26 percent users installed total security, 3.65 percent users installed internet security and only a few 3.39 percent users installed home edition.
    - It was seen that, only 9.64 housewives installed antivirus tool on their personal computer, out of which 9.64 percent house wives installed total security antivirus tool. It was also seen that house wives haven't installed internet security and also home edition antivirus tool on their personal computers.(Table No.4.17)
13. It was seen that 63.30 percents users said that updating of antivirus tool done automatically and 53.40 percent users said that full system scan done automatically. (Table No. 4.18).
    - It was observed that 4.70 percent users updating antivirus tool daily and 10.20 percent users does the full systems scan daily.
    - It was seen that, 7.80 percent users update antivirus tool weekly and 19.30 percent users do the full system scan at least once in a week.
    - It was found that, 18.80 percent users update antivirus tool monthly and 4.90 percent users do the full systems scan at least once in a month.
    - It was seen that very few that is 5.20 percent users update antivirus toll occasionally when they remember and 2.90 percent users do the full system scan occasionally when they remember.
    - It is also observed that only 0.30 percent users not dong updating of antivirus tool and 7.80 users not scanning full system.

14. It was clear that 92.70 percent users used paid version whereas only a few that is 7.30 percent users used free version of antivirus tool.(Table No. 4.19)
15. It was observed that 61.50 percent users doing financial transactions by using their personal computer whereas 38.50 percent users not doing financial transaction manually by going in bank(Table No. 4.20)
16. It was observed that 80.46 percent users have not suffered any financial loss due to virus but a 19.56 percent user had faced financial loss due to virus before using of antivirus tools.(Table No. 4.21)
17. It was seen that around 54.90 percent users imposed restrictions by using antivirus tools to avoid attacks whereas 45.10 percent users has not placed any restrictions.(Table No. 4.22)
18. It was seen that around 60.90 percent users personal computers/Laptops/Mobile phones are protected with antivirus tools whereas 39.10 percents users personal computers/Laptops/Mobile phones are not protected with antivirus tools.(Table No. 4.23)
19. It was seen that highest average value is 4.03 for Service provided by the help/support center followed by Procedure of Virus Database Definition Update is 4.00 and Procedure of Version Update is 4.00. All these three indicate the status of the present antivirus tools used by the user and moreover due to support of service provider, virus database and version are very much satisfied to the user. (Table No. 4.24)
20. Based on primary data, users are satisfies with help /support provided by the service provider and it got First rank with weightage of 72.13 percent. It was followed by Second rank for 'Virus Database Definition update' with weightage of 70.57 percent. Finally Third rank is for 'Procedure of Version Update' with weightage of 65.36 percent. According to these it clear, users are very much satisfied with present antivirus tools which they are using.(Table No.4.24)
21. The various types of services provided by help/support center of present antivirus tools like online support, support through email, telephonic support, user forum and user manual/trouble shooting manual are assessed and ranked. To meet the objective question is designed by using various parameters which defines the status of services provided antivirus company's support center. It was seen that highest average value is 4.16 for 'Online Support' followed by 'Support through email with average value is 4.11, for 'telephonic support' with average value is

4.04, for user forum average value is 4.02 and further for User manual / Trouble hooting manual is 4.01. All these five indicate the help/support center services to the user of the present antivirus and moreover due to support of service provider most of the user are very much satisfied to the user. (Table No. 4.25)

22. The various parameters of scanning capability of the present Antivirus Tool are assessed.. To meet the objective question is designed by using various parameters which are important for security of personal computer. It was observed that for each parameter average scale is in-between 1 to 5 that is in-between Excellent to poor. In fact all are above 3.5 which mean that with respect to all the parameters much improvement is observed. It was seen that highest average value is 4.24 on-access scanning followed by scheduled scanning is 4.08 and compressed files scanning is 3.92. All these four indicate that scanning capability of present antivirus tool is high and users are very much satisfies with present antivirus tool. Apart from these benefits it is observed that average value for registry startup protection is 3.90 followed by 3.89 for manual scanning 3.88 for email protection, 3.87 for quarantines infected files,3.85 for on-demand scanning, 3.84 for web mail protection, 3.83 for Auto-Clean infected files. Further also average value for ad ware/Spyware scanning is 3.73, 3.62 is for file sharing, 3.56 is for Heuristic scanning whereas 3.52 is for Script blocking and further 3.51 for instant messaging protection.(Table No. 4.26)
23. The various parameters of settings of antivirus tools done by the user. It includes parameters like, Scan Scheduling, Password Protect Settings, Parental Control, Files and Folders, External drivers and devices, Internet & Network and Emails. To meet the objective question is designed by using various parameters which defines the scanning status of antivirus tools. It was seen that highest average value is 2.83 for 'On Scan scheduling' followed by 'External drivers and devices' and Internet & Network' with average value of 2.83. Also average value of 'emails' is 2.74, followed by 'Password Protect settings' with average value was 2.71, for 'Files & Folders' is 2.70 and further for 'parental control' with average value is 2.44. All these seven indicate the setting status of the present antivirus tool to the user . (Table No. 4.27)
24. It was cleared that most of the users that is 56.77 percent, tighten the privacy settings of facebook on monthly basis followed by weekly is 19.79 percent, 11.20 percent doing it occasionally whereas 6.51 percent is yearly and 5.73 percent user

doing it daily. (Table No.5.28). So Ratio of Tightened privacy setting in your facebook monthly is higher than that of daily, weekly, yearly and occasionally.

- It was seen that most of the users that is 56.77 percent, Change passwords of net banking on monthly basis followed by weekly is 19.79 percent, 11.20 percent doing it occasionally whereas 6.51 percent is yearly and 5.73 percent user doing it daily. Ratio of change of password of net banking is higher than that of daily, weekly, yearly and occasionally. (Table No.4.28)
- It was seen that most of the users that is 52.08 percent, Chang email password on monthly basis followed by weekly is 21.35 percent, 11.20 percent doing it occasionally whereas 8.59 percent is daily and 6.77 percent user doing it yearly. Ratio of monthly change password of email is higher than that of daily, weekly, yearly and occasionally. (Table No.4.28).
- It was found that, 44.27 percent users take backup of their data occasionally followed by 27.60 percent yearly and 14.06 percent users take backup of data weekly and monthly and further no one take backup of their data on daily basis.(Table No.4.28)
- It was seen that most of the users that is 58.33 percent, Change the security settings of browser occasionally followed by 23.18 percent yearly, 11.46 percent doing it monthly whereas 7.03 percent is weekly and no one is on daily basis. Ratio of Change in browser security setting done occasionally is higher than that of daily, weekly, monthly and yearly. (Table No.4.28).
- Also 74.74 percent users change the security setting of operating system occasionally followed by 25 percent users doing it yearly and a very few that is 0.26 percent doing it monthly. Whereas no one is doing the setting of operating system on daily and weekly basis. (Table No.4.28)

25. The various parameters of importance of antivirus tools to understand quality parameters and capability of the present Antivirus Tool are studied. it was observed that average value for Security is 4.78 followed by Malware detection is 4.55, followed by Firewall Security is 4.52, 4.34 is for Ease of use and 4.25 is for update frequency. Further average value of database size is 4.15 followed by for safe banking is 4.11, for activity reporting is 4.10, for effect on system speed is 4.08 and also 4.01 for scanning speed, 4.00 is for startup protection. Further average value of Cost is 3.98 followed by registry is 3.93 whereas P2P/File

sharing protection is 3.92, overall size in bytes is 3.90, Licensed arrangements is 3.89, web-page scanning/anti-phishing is 3.82 and free additional software is 3.4. (Table No. 4.29)

26. It was observed that 96 percent users are satisfied antivirus tools whereas remaining 4 percent users are dissatisfied. According to these ratios, it shows that users are aware about the security of personal computer so that they are highly satisfied with antivirus tools.(Table No. 4.30)
27. It was seen that 96.35 percent users are satisfied out of which 55.99 percent working professionals are satisfied with antivirus tools followed by 32.55 percent Student users are satisfied and 9.64 percent housewives are satisfies with antivirus tools. Only 3.65 users are not satisfied in which 1.82 percent working professionals and students. It is shows that all users are very much satisfied with all features of antivirus tools.(Table No. 4.32)
28. It was observed that 57.81percent users are satisfied with quick heal antivirus because it is supported various important features such as parental control, antimalware, USB drive protection, database security has proved that Quick heal is most popular antivirus. From primary data it is clear that 49.22 percent users are satisfied with Net protector antivirus, its cost is very less as compared to other antivirus and it also support important features. It is followed by 18.75 percent users are satisfied with McAfee Virus. A very low satisfaction ratio for next antivirus is 18.49 percent for Kaspersky antivirus. Still 13.02 percent users are satisfied with Norton antivirus and lastly 12.24 percent are satisfied with AVG antivirus.(Table No.4.33)

5.2.2 Part II: Findings related to Vendors of Antivirus Tools

1. It was seen that most of the antivirus tools Quick Heal, Norton &Net Protector are sold Mostly. It is followed by McAfee sold by 89 percent Further, Kaspersky & AVG sold by 27 percent. So Maximum sale of Antivirus tools like Norton,McAfee & Net protector is observed because performance, service and cost.(Table No.4.34).
2. It was seen that most of the user are using Total security product (100 percent) .It is followed by Internet security product is 46 percent. Further, antivirus product is 10 percent. It is seen that, popular product is total security. (Table No.4.35).

3. It was seen that 100 percent users purchased antivirus tool protecting single device for single year. Further, single device for multiple year protection is purchased by 32 percent. It is seen that, 46 percent of users purchased protection for multiple device multiple year saving money and securing the complete personal computer system (Table No. 4.36)
4. It has been observed that, Kaspersky,AVG,Nortn,QuickHeal &McAfee antivirus tools are having price between Rs.501 to Rs.1000 and it supporting Single Device Annually. KasperSky, AVG antivirus tools having cost between Rs.501 to Rs.1000 and Quick Heal having cost is Rs.1001 to Rs.1500 and it supporting Multiple Device Annually.
    - Kaspersky Internet security 1 device 3 years having cost is Rs.1001 to Rs.1500 and Quick Heal Internet security 1 user 3 years cost is more than Rs.2000 and theses Internet security tools are supporting for Single device & multiple years. Kaspersky Internet security (3 pcs) and Norton security Deluxe (5 devices) having cost is Rs.1501 to Rs.2000, AVG Protection PRO (unlimited PCS), McAfee Internet security1 year unlimited devices having cost is Rs.1001 to Rs.1500 and Quick Internet security 3 users 1 year having cost is more than Rs.2000 and supporting Multiple device annually.
    - The Total security products are like Kaspersky Total Security 3 PCS, Norton Security Premium (10 devices), McAfee Total Protection 1 year unlimited devices, & Quick Heal Total Security 3 users 1 year having cost is more than Rs.2000 and AVG Ultimate (Unlimited Installations) having cost is Rs.1501 to Rs.2000 where as Net Protector Total Security 3 PCS having cost is Rs.501 to Rs.1000/-(Table No.4.37).
5. It was seen that highest scale for Kasper Sky are for Best Performance and Services (4.59) and Low cost (1.46).It is followed by Norton antivirus tools highest scale for Best Performance and Services (4.59) and Low cost (1.46). AVG antivirus tools highest scale for Best Performance (4.59)**,** Services (4.30) and Low cost (1.46). McAfee antivirus tools highest scale for Best Service (4.3)**,** Best Performance (3.51) and Low cost (1.41). Quick Heal antivirus tools highest scale for Best Performance and Services (4.84) and Low cost (1.46).It is followed by Net protector highest scale for Low cost (5),Best Service (4.27) and Best Performance (4.00) .(Table No. 4.38)

6. It was seen that, all kind of services such as (online support, telephonic support, remote support and email support) are provided by Antivirus Company (100 percent) to users after purchasing antivirus tool.(Table No.4.39).
7. It is clear that 99 percent user is satisfied with the Online Support and Telephonic support. It is followed by 96 percent user satisfied with Email Support and 90 percent users are satisfied with remote service. (Table No.4.40)

5.3 Conclusions

This paragraph presents the conclusion arising out of the study. Based on the primary data we found that most of the users complaint about virus attack and most of them used antivirus tool to safeguard their computer. This showed that users are aware about the problems caused by viruses and also the importance of antivirus. We also concluded that users has better knowledge about viruses and used antivirus tools of different companies and types.

1. **Distribution of antivirus users according to Gender :** Ratio of male users is slightly higher than female respondents. Means in the era of Information Technology, still most of the internet users are male as compared to the female users and they dominate females in this sector.
2. **Distribution of antivirus users according to their Educational Qualification:** It is apparent that most of the users are highly educated. When a comparison between types of users, house wives are less educated and working professionals and students are highly educated.
3. **Distribution of antivirus users according to their types:** Contribution ratio in study of working professionals is high as compared to the Students and Housewives.
4. **Awareness of Antivirus Tool among the personal computer users:** Awareness of the all users about antivirus Tools is very high so we can conclude that users are aware about security of personal information and personal data also.
5. **Distribution of User wise awareness of Antivirus Tool:** Ratio of awareness of antivirus tools for their personal computers among the working professionals is very high as compared to the students followed by housewives.

6. **Selection criteria for purchase of Antivirus Tool:** Most of the users prefered brand while purchasing antivirus tool followed by price and service. So we can say that brand is of antivirus tool has a very much positive impact on user.
7. **Edition of Antivirus Tool:** Most of the user used licensed edition of antivirus tools as compared to the free/trial edition of the antivirus tools. It clears that users are ready to pay for securing their data and personal details and indirectly aware about importance of antivirus tools.
    a. Very high usage of licensed edition of antivirus tools by the user followed by trial and both the editions.
    b. Working professionals are highly aware about security and due to that they mostly preferred licensed edition of antivirus tools followed by students also.
    c. Response from housewives is very low as compared to the working professionals and students.
8. **Usage of Antivirus Tool:** Most of the users uses Quick heal as a high security reason as compared to the other antivirus tools like Net Protector, McAfee, Kaspersky, Norton and AVG.
9. **User wise Usage of Antivirus Tool:** Most of the working professionals and students are highly used Quick heal antivirus tools followed by Net Protector, McAfee, Kaspersky, Norton and AVG antivirus tools for security reason whereas house wives use only Net Protector and Norton Antivirus tool as compared to other tools.
10. **Cost wise Usage of Antivirus Tool:** Most of the users prefers that cost of antivirus tools below Rs. 1000/- followed by cost of range in between Rs. 1001/-to Rs. 1500/- and further range in between Rs.1501/- to Rs. 2000/-. Only a few users can afford amount of Rs. 2001/- to Rs. 2500/- and more than Rs. 2500/-. So it clears that user wants best security in less cost.
    a. Net Protector is highly purchased by the user followed by Quick Heal, McAfee, Kaspersky, Norton & AVG in cost range less than Rs. 1000/-.
    b. It range of cost Rs. 1001/- to Rs. 1500/- and Rs.1500/- to Rs.2000**/-,** most of the users purchase Quick Heal followed by Net Protector, McAfee, Kaspersky and Norton & AVG.
    c. In between range cost Rs.2001/- to Rs. 2500/-, users only purchase Quick Heal not any other antivirus tools.

d. For cost more than Rs.2500/-, users purchase only Quick Heal, Net Protector, McAfee & Kaspersky but not Norton and AVG.

11. **Type of Antivirus Tool:** It is seen that most of the users prefers to use total security antivirus tool as compared to the internet security and home edition.
12. **User wise and Type wise Usage of Antivirus Tool:** It is seen that working professionals and students are highly used total security antivirus tool on their personal computer followed by internet security and home edition. Only a few house wives used only total security not a internet security and home edition.
    a. Ratio of usage of total security among working professionals followed by students is very high as compared to the house wives. Usage of internet security and home edition among house wives is absolutely not any.
13. **Update and scanning frequency of Antivirus Tool:** It was observed that most of the users depend on automatic updating and scanning of antivirus tool when they start their personal computer.
    a. It is also observed that most of the users update antivirus tool at least once in a month followed by at least once in a week, occasionally when they remember, daily and then no updation.
    b. Users does the full system scan of personal computer at least once in a week followed by daily, never does the scanning, at least once in a month and Occasionally when they remember.
    c. Ratio of updation of antivirus tool is little bit higher than of scanning of full system.
14. **Version of Antivirus Tool:** Ratio of paid version users is higher than that of free versions so it conclude that the most of the users are highly aware of their data and its security and due to that reason using paid version instead of free version of antivirus tools.
15. **Ration of doing financial transaction on Personal computer:** Ratio doing financial transaction by user is higher than the ratio of users doing financial transaction manually by visiting in bank.
16. **Ratio of users suffering financial loss due to virus:** Ratio of users suffered financial loss is very low and it clears that might be users are aware about threats and while during financial transaction they check for secure website

like https:/ instead of http:/ with padlock symbol. So here we can say that awareness regarding security among the user is high.

17. **Imposition of restrictions done by the users:** Imposition of restrictions done by the user to avoid virus attack is higher than that of non imposition of restrictions. By looking at the ratio of not placing restrictions on the user to avoid virus attack, need to create awareness about threats, attacks etc. and their security settings.
18. **Number of devices protected by antivirus tool:** Protection of all devices like /laptops/mobile phones/tablets by antivirus tool with respect to the users is higher as compared to the partially protected devices with antivirus tools. So we can conclude that most of the users are aware about protection of their personal computers/Laptops/Mobile phones and accordingly they take care of all devices.
19. **Services provided by antivirus tool:** Based on primary data, users are satisfied with help /support provided by the service provider and it got First rank followed by Second rank for 'Virus Database Definition update' and finally Third rank is for 'Procedure of Version Update', so we conclude that users are very much satisfied with present antivirus tools which they are using.
20. **Services provided by antivirus company support center:** Based on primary data, users are satisfied with 'online support' and it got First rank Second rank for 'Support through email', third rank is for 'Telephonic support', second last rank that is fourth rank is for 'User Forum' and further last rank is for 'User manual / Trouble hooting manual', so we conclude that users are very much satisfied with present antivirus tools which they are using and support provided by the vendor.
21. **Scanning capability of antivirus tool:** Based on primary data, users are satisfied with 'On-access scanning' and it got First rank Second rank for 'scheduled scanning', third rank is for 'compressed file scanning', fourth rank is for 'registry startup protection' and further fifth rank is for 'manual scanning'. Further sixth rank is for 'email protection', seventh rank is for 'quarantines infected files', so we conclude that users are very much satisfied with present antivirus tools which they are using and support provided by the vendor. Eighth rank is for 'on-demand scanning' followed by ninth rank is for

'web mail protection', Tenth rank is for 'Auto-Clean infected files', eleventh rank is for 'ad ware/Spyware scanning', Twelve rank is for 'file sharing', thirteenth rank is for ' Heuristic scanning' and second last that is fourteenth is for 'Script blocking' and last that is fifteenth is for 'Instant messaging protection'.

22. **Management of antivirus tool by user:**It is seen that highest average value is for 'On Scan sceduling' followed by 'External drivers and devices' and Internet & Network', 'emails' ,'Password Protect settings' ,'Files & Folders' and further for 'parental control'. All these seven parameters indicate the setting status of the present antivirus tool to the user and which is highest and help for user satisfaction.
23. **Frequency of changing settings of antivirus tool:** Most of the user change the setting of facebook, operating system and browser occasionally as compared to the weekly and yearly.
    a. Most of the users are changing the password of email, net banking occasionally followed by monthly, weekly, daily and yearly.
24. **Important parameters in antivirus tool:** As per the users point of view, important parameters of antivirus tools and their first preference is for 'Security' parameter as they have ranked it First followed by Second rank is for 'Malware Detection', Third rank is for 'Firewall security', fourth rank is for 'Ease of use', fifth rank is for 'Update frequency', sixth rank is for 'database size' whereas seventh rank is for 'safe banking', eighth rank is for 'activity reporting' followed by ninth rank is for 'Effect of System Speed' and tenth rank is for 'Scanning speed'. Further it is seen that eleventh rank is for 'start-up protection' followed by twelfth rank is for 'cost', thirteenth rank is for 'Registry', fourteenth rank is for 'P2P/File Sharing Protection' whereas fifteenth rank is for 'Overall size in bytes', sixteenth rank is for 'Licensed Agreements', seventeenth rank is for 'Web-page Scanning/Anti-Phishing' and further last means eighteenth rank is for 'free additional software'.As per the responses, it is clear that users are satisfied with antivirus tools keep safely for performing day to day to activities.
25. **Measurement of satisfaction about the antivirus tool:** Satisfaction among the user about current usage of antivirus tool is very high as compared to the

dissatisfaction. It can be concluded that the users are highly satisfied with antivirus tools.

26. **Company wise satisfaction of antivirus Tool:** Quick Heal is highly favorable among the users followed by Net protector. McAfee ,Kaspersky, Norton, and last one AVG.
27. **Popular antivirus tools :** Maximum sale of antivirus tools of Quick Heal, Net Protector and Norton followed by McAfee, and further sale of antivirus are Kaspersky & AVG.
28. **Popular type of antivirus product :** Popular antivirus product among the users is total security followed by internet security and further antivirus product. So it is seen that maximum usages of popular product is total security.
29. **Purchase Pattern of package of antivirus tool:** It is seen that Single device for single year pattern is purchased mostly by users followed by multiple device for single year package and further single device for multiple year package are also purchased. So it is seen that maximum users are purchased single device for single year.
30. **Reason behind the popularity of antivirus company:** As per user's point of view,
    a. Net Protector antivirus tool has low cost and best performance as compared to other antivirus tools.
    b. Most of the users agreed that 'Quick Heal' is popular for best performance and best service.
31. **Services provided by antivirus company :** Most of antivirus companies help/support centers are providing full support like telephonic, online as well also through e-mail support to antivirus users.

5.4. Suggestions

For a better tomorrow we need to have a better today and so if want to secure digital life by protecting personal computer from virus attacks by using antivirus tools. Consideration of the users problems for maintaining security of personal computer, need to management of antivirus tools in a way which will protect personal computer from threats and viruses and find it easy to implement it.

Following are some suggestions for the successful management of security of personal computer by using antivirus tools.

A) Suggestion for Users of antivirus tools

To thoroughly understand this, consider an example of home security. Home security can be achieved by using a lock at door when you are going out of home.

Figure 5.1 Complete House protection

But only using lock you cannot prevent home robberies along with that you can take following precautions also.

- **Top 10 security tips to prevent a home robbery.**

1. Get an Indoor Dog
2. Lock your doors, garage as well as windows also
3. Build a fence
4. Keep shrubbery around entrances and walkways trimmed
5. Get to Know your neighbors
6. Install an alarm or motion sensors
7. Hide valuables
8. Install double key Deadbolts
9. Don't advertise about your vacation plan
10. Be suspicious of door knockers and marketers

In this example lock is like an antivirus tool. Even though you are using a lock we need to follow above tips to protect out home from robbery. In similar manner every personal computer user using antivirus tool has to adopt following 21 tips to attain the personal computer security.

Figure 5.2 Complete PC Protection

- **Top 21 security tips for antivirus users**

1. Use licensed antivirus tool and update it regularly. Don't rely on the automatic update and tighten the antivirus settings
2. Use uppercase, lowercase and special characters and numbers in your every password and also change the password of email accounts/bank accounts and facebook account periodically to protect personal identity and to avoid data and/or money theft and reputation loss.
3. Use patched, up to date browsers and configure the setting of browser to high security. (Refer annexure 7)
4. Download free software only from verified publishers. If you download a file online ensure that you check it's extension before clicking on it.
5. While giving your personal information or shopping or banking online ensure that url begins with 'https' and is accompanied by padlock symbol.
6. Use secure browsing on facebook and tighten privacy settings on facebook.(Refer annexure 6).
7. Accept friend request only from people you know personally.
8. Be Vigilant .If you get a windows pop up that looks like it's scanning your hard drive for viruses or errors, yet you have never observed this program before, close it immediately.
9. Use two step verification for your email account and also tighten it's security settings (Refer Annexure 8)
10. It is observed that users are taking back up of data occasionally. Always take backup of your data.
11. Never visit banking/shopping sites/ social sites via email.
12. Never shop or bank using unsecured wifi networks.

13. Avoid using official email address for social media sites or any other websites other than that of your organization.
14. Delete old and inactive accounts.
15. Don't make your photos/videos public on internet keep them visible only to people you acquainted.
16. Increase your knowledge about cyber threats and cyber security.
17. Don't save your credit/debit card information on websites.
18. Change your online banking password every six months and check your bank statements regularly.
19. If you are buying from unfamiliar website, then go to cash on delivery option.
20. Secure wireless network at home by changing its default password and using WPA2 encryption
21. If you get an email from bank asking username and password then make a call to bank

B) Suggestions to conduct Awareness programs on Security of Personal Computer for users of antivirus tool: Security begins with a simple message everyone using the Internet along with antivirus tool can adopt that is to take security and safety precautions, settings of antivirus tool and understand the consequences of the actions and behaviors. For this awareness about security of personal computer is a must.

- Awareness can also be done by using traditional methods using media vis. namely radio, television, newspaper etc.
- To make a complete system virus proof, it is required that the settings of antivirus tool, browser, operating system should be tightened. But it is observed in study that users are configuring the settings occasionally followed by monthly, weekly and daily. Need to create awareness about threats come from Wi-Fi internet services among the users and how to prevent it by tightening the settings of antivirus tool, browser, operating system. So such kind of awareness programs about security of personal computer can also be arranged by vendor and antivirus tool companies to support users.

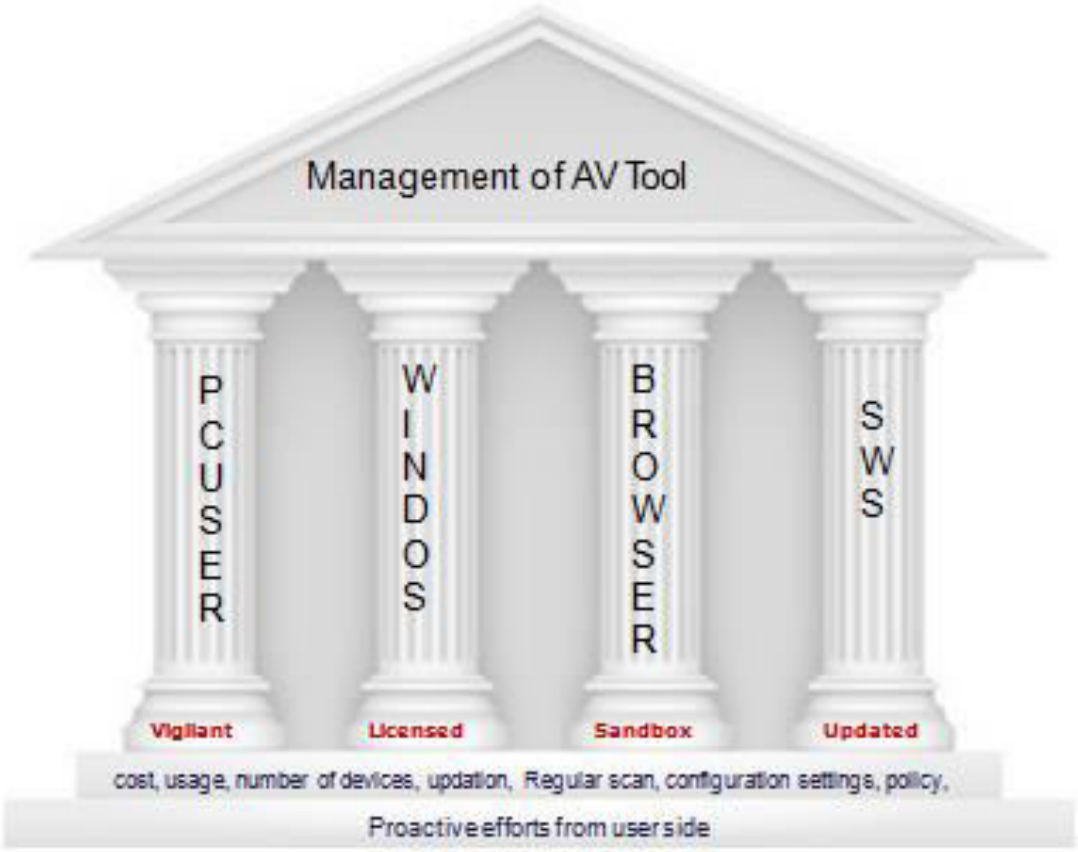
- Create awareness regarding usage of licensed copy instead of free/trail copy of antivirus tool because the free of trial copy may be the small version providing basic protection while licensed copy will provide full protection.
- As per primary data, brand plays important role for usage of antivirus tool among the user, so antivirus company can create awareness by branding their product innovatively.

C) Training programs for Vendor: Lack of proper management of antivirus tools, settings of antivirus tools and security training for vendor could create security breaches in user personal computers.

- Security setting awareness and training should be made part of the rules and regulations while selling the antivirus tools of vendor.
- For this purpose it should be mandatory for all vendors to undergo a security management training of antivirus tools which should be provided by the Companies at free of cost.

Suggested Model (Figure 5.3)

This is suggestive action plan for management of antivirus tool so that to attain



personal computer security from all the internet treats and malwares.

1) Every personal computer users should be always vigilant because virus can enter through the attachments, pirated softwares or through networks. Responsible behavior of user is very important to maintain digital hygiene.
2) Always use licensed windows operating system because it will be always updated for current malware threats. Otherwise hawkers may exploit this opportunity.
3) Always use browser in sanbox environment means it creates virtual environment and executes your browser in this environment hence any file you download or gets downloaded from browser remains in isolated in sandbox environment. So infection will remain confined in this virtual environment without affecting real PC. And once you close the browser any changes that might have occurred in environments will be deleted.
4) Always use the updated versions of all softwares you are using otherwise they will provide loop holes to the cyber criminals.
5) Management of antivirus tool refers to policies related to selection, installation, updating and renewal of antivirus tool. While selecting antivirus tool user has to consider cost, number of devices to be protected, number of years to be protected and the usage of computer. Users should update the antivirus tool regularly and should scan the whole system frequently.

   Hence the user policy, control, review, security awareness, operational procedures play important role in the management of antivirus tool.

5. 5 Scope for future Research

Security is a broad field. Lots of work can be studied in the future. Over time, the variety and sophistication of network attacks are likely to increase. Thus there is requirement for ongoing research in this field that can cater for the new challenges. Since in depth studies in these areas have long term social-economic dimension and repercussions, the scope of the investigation can be further expanded as follows:

- Due to limitation of time in obtaining data from users the work has been restricted to geographical areas of Pune city. Rural area can be considered

for further research which can be more useful, informative and illuminating.

- Researcher could have studied other types of users and their problems related to cyber security. Further research can be taken to study government officials and police authorities' perspective and problems related to security implementation.
- The researcher has considered routine users problems related to security, further study related to other public places where internet services are provided such as Hotels, Restaurants, and Airports etc. can be considered.
- Further research can also be focused on the role of antivirus tools in controlling and eradicating threats and virus attacks.

Annexure 1

Questionnaire for Users survey

Note: The questionnaire is prepared to collect information related to evaluate performance of anti-virus tools for Personal Computers in Pune city for the purpose of research work.

The contents of this form will be treated as strictly confidential and used for academic purposes only.

Q.1. Name (Optional):_____

Q.2. Types of user

A. Working Professionals B. Students C. House Wives

Q.3. Are you aware about anti-virus tools?

A. Yes **B.** No

Q.4. What type of Anti-virus tools package are you using?

A. Trial **B.** Licensed

Q.5. Which anti-virus software is being used by you?

A. Kaspersky anti-Virus **B** Norton anti-Virus

C. Avg anti-Virus **D** McAfee Virus scans

E. Quick Heal anti-Virus **F** Net Protector

G. Other(give name):

Q.6. Which type of anti-virus tools installed on your PC?

A. Total Security B. Internet Security C. Home Edition D. Any Other

Q.7.How often do you update your anti-virus software?

A. It is done automatically

B. Daily

C. At least once a week

D. At least twice a week

E. At least Once a month

F. Occasionally, when I remember

G. Never

Q.8.How often do you perform a full system anti-virus scan?

A. It is done automatically
B. Daily
C. At least once a week
D. At least twice a week
E. At least Once a month
F. Occasionally, when I remember
G. Never

Q.9. Do you have anti-virus software installed on your computer?

If you do, did you pay for your anti-virus software or is it a free version? *

- Yes Paid version
- Yes Free version
- No
- Don't know

Q.10 Are you satisfied with current Antivirus Tool?

A)

A. Yes **B.** No

B) If Yes-

Please rate your software on a scale of 1 to 5, where 1 means you are satisfied with the tools, and 5 means you are dissatisfied with the tools very much

Level of Satisfaction	1	2	3	4	5
	◉	○	○	○	○

Q.11.Rate the following the parameters which you think are important in an antivirus software (Rate them on an importance scale of 1 to 5 where 1 is the most important and 5 is the least important)

	1	2	3	4	5
Security	☐	☐	☐	☐	☐
Malware detection	☐	☐	☐	☐	☐
Firewall security	☐	☐	☐	☐	☐
Web-page scanning/ anti-	☐	☐	☐	☐	☐

phishing					
Scanning speed	☐	☐	☐	☐	☐
Update frequency	☐	☐	☐	☐	☐
Registry startup protection	☐	☐	☐	☐	☐
Cost	☐	☐	☐	☐	☐
Database size	☐	☐	☐	☐	☐
Overall size in bytes	☐	☐	☐	☐	☐
Free additional software	☐	☐	☐	☐	☐
Effect on system speed	☐	☐	☐	☐	☐
Licensing arrangements	☐	☐	☐	☐	☐
Activity Reporting	☐	☐	☐	☐	☐
Ease Of Use	☐	☐	☐	☐	☐
P2P/File Sharing Protection	☐	☐	☐	☐	☐
Safe banking	☐	☐	☐	☐	☐

Q.12. On which priority basic you select the security product?

A. Brand Name B. Service C. Cost

Q.13. Total cost of anti-virus software purchased by you?

A. Less than Rs. 1000 **B** Rs. 1000 to 1500

C. Rs. 1501 to 2000 **D** Rs. 2001 to 2500

E. More than Rs. 2500

Q.14. A. Are you doing any financial transaction on personal computer?

A. Yes **B.** No

B. If Yes,

A. With Antivirus Tool **B.** Without Antivirus Tool

Q.15. Did you experience any financial loss due to Virus attack on your computer system before using Anti-virus software?

A. Yes **B.** No

Q.16**.** Have you imposed any restrictions on the user to avoid virus attack?

A. Yes **B.** No

Q.17. Are all your computers / Laptops/mobile phones protected by anti-virus software

A. All **B.** Partly Protected

Q.18**.** Please specify the rates for the present anti-virus software

Sr. No	Antivirus Tools	Excellent [5]	Very Good[4]	Good [3]	Poor[2]	Fair[1]
1	Service provided by the help/support center					
2	Procedure of Virus Database Definition Update					
3	Procedure of Version Update					

Q.19.Rate the following aspects related to the technical support of the present Anti-virus Software?

Sr. No	Aspects related to the technical support	Excellent [5]	Very Good[4]	Good [3]	Poor[2]	Fair[1]
1	Online support					
2	Telephonic support					
3	Support through Email					
4	User manual / Trouble hooting manual					
5	User Forum					

Q.20.Rate the following aspects related to the scanning capability of the present anti-virus software

Sr. No	Aspects related to the scanning capability of the present anti-virus software	Excellent [5]	Very Good[4]	Good [3]	Poor[2]	Fair[1]
1	On-access Scanning					

2	On-demand Scanning					
3	Scheduled Scanning					
4	Manual Scanning					
5	Compressed Files Scanning					
6	Auto-Clean Infected Files					
7	Email protection					
8	File Sharing protection					
9	Web Mail protection					
10	Heuristic Scanning					
11	Ad ware / Spyware canning					
12	Script Blocking					
13	Quarantines Infected Files					
14	Instant Messaging protection					
15	Registry Startup Protection					

Q.21. What is your opinion about the Settings of present anti-virus software?

Sr .No	Types of Setting	Satisfactory	Can‘t Say	Not Satisfactory
1	On Scan Reporting / History			
2	Password Protect Settings			
3	Parental Control			
4	Files and folders			
5	External drives and devices			
6	Internet and network			
7	Emails			

Q.22.Which services antivirus company provide to the user after purchasing?

Sr.No	**Support After Purchasing**	**Yes**	**No**
1	Onsite support		
2	Telephonic support		
3	Remote support		
4	Email support		

Q.23 If you get an email from bank asking for your username, password and ATM pin, what would you do? (For s/w professionals A 2% B 38% C 60%)

A. Provide the asked information
B. Ignore that mail
C. Report the mail immediately to the bank

Q.24. Do U trust unknown emails that ask you to click links or download attachments or advertisements?

A) Yes B) Partially C) No

Q. 25. Rate the Following Parameters

Factor	**Daily**	**Weekly**	**Monthly**	**Yearly**	**Occasionally**
Tightened privacy setting in your facebook					
Change your passwords of net banking					
Change your passwords of net banking					
Take backup of your data					
Change the security settings of our browser					
Change the security settings of operating system					

Q.26.Please give your comments in 2 -3 lines about your overall experience of using the Anti-virus Tools. **[OPTIONAL]**

Annexure 2

Questionnaire used for Antivirus/Computer (Vendors/Assemblers)

This questionnaire is drafted as a part of research trying to find out the use of antivirus for personal computer.

(Please tick appropriate option according to your experiences)

Name (optional):_____

Name of Organization:_____

Email/Mobile: _____

Q.1 Which is antivirus tool you sold?

A. Kaspersky anti-Virus **B** Norton anti-Virus

C. Avg anti-Virus **D** McAfee Virus scans

E. Quick Heal anti-Virus **F** Net Protector

G. Other(give name):

Q.2 Which is antivirus tool u sold Mostly?

A. Kaspersky anti-Virus **B** Norton anti-Virus

C. Avg anti-Virus **D** McAfee Virus scans

E. Quick Heal anti-Virus **F** Net Protector

G. Other(give name):

Q.3.Which types of antivirus products are popular?

a) Antivirus b) Internet Security c) Total Security

Q.4. Which antivirus products are purchased mostly?

a) Supporting single device single year

b) Supporting single device multiple years

c) Supporting multiple devices single year

d) Supporting multiple device multiple years

Q.5.Please Specify the cost of antivirus products supporting Single device annually.

Sr. No	Antivirus Tools	Less than Rs. 500	Rs. 501 to 1000	Rs. 1001 to 1500	Rs. 1501 to 2000	More than Rs. 2000
1	Kaspersky anti-Virus					
2	Norton Security Standard					
3	AVG anti-Virus					
4	McAfee Antivirus Plus					
5	Quick Heal anti-Virus Pro					

Q.6. Please Specify the cost of antivirus products supporting Multiple device annually.

Sr. No	Antivirus Tools	Less than Rs. 1000	Rs. 1000 to 1500	Rs. 1501 to 2000	Rs. 2001 to 2500	More than Rs. 2500
1	Kaspersky anti-Virus					
2	McAfee Antivirus Plus					
3	Quick Heal anti-Virus Pro					

Q.7.Please Specify the cost of Internet security products supporting Single device annually.

Sr. No	Antivirus Tools	Less than Rs. 1000	Rs. 1000 to 1500	Rs. 1501 to 2000	Rs. 2001 to 2500	More than Rs. 2500
1	Kaspersky Internet security 1 device 1 year					
2	AVG Internet security					
3	Quick Heal Internet security 1 user 1 year					

Q.8.Please Specify the cost of Internet security products supporting Single device & multiple years

Sr. No	Antivirus Tools	Less than Rs. 1000	Rs. 1000 to 1500	Rs. 1501 to 2000	Rs. 2001 to 2500	More than Rs. 2500
1	Kaspersky Internet security 1 device 3 years					
2	Quick Heal Internet security 1 user 3 years					

Q9. Please Specify the cost of Internet security products supporting Multiple device annually.

Sr. No	Antivirus Tools	Less than Rs. 1000	Rs. 1001 to 1500	Rs. 1501 to 2000	Rs. 2001 to 2500	More than Rs. 2500
1	Kaspersky Internet security (3 pcs)					
2	Norton security Deluxe (5 devices)					
3	AVG Protection PRO (unlimited PCS)					
4	McAfee Internet security 1 year unlimited devices					
5	Quick Internet security 3 users I year					

Q.10.Please Specify the cost of Total Security products supporting Single device annually.

Sr. No	Antivirus Tools	Less than 500	Rs. 501 to 1000	Rs. 1001 to 1500	Rs. 1501 to 2000	Rs. 2001 to 2500	More than Rs. 2500
1	Kaspersky Total Security						
2	Quick Heal Total Security 1 user 1 year						
3	Net Protector Total security						

Q.11. Please Specify the cost of Total security products supporting Multiple device annually.

Sr. No	Antivirus Tools	Less than Rs. 1000	Rs. 1000 to 1500	Rs. 1501 to 2000	Rs. 2001 to 2500	More than Rs. 2500
1	Kaspersky Total Security 3 PCS					
2	Norton Security Premium (10 devices)					
3	AVG Ultimate (Unlimited Installations)					
4	McAfee Total Protection 1 year unlimited devices					
5	Quick Heal Total Security 3 users 1 year					
6	Net Protector Total Security 3 PCS					

Q.12.Which service you provide while selling the Antivirus Tools?

Sr. No	Antivirus Tools	While Purchasing
1	Operating System Setting	
2	Browser System Setting	
3	Automated Updation Setting	
4	Antivirus tool setting	

Q.13.Which services Antivirus company provide to users after purchasing the antivirus tool?

1. Onsite support
2. Telephonic support
3. Remote support
4. Email support

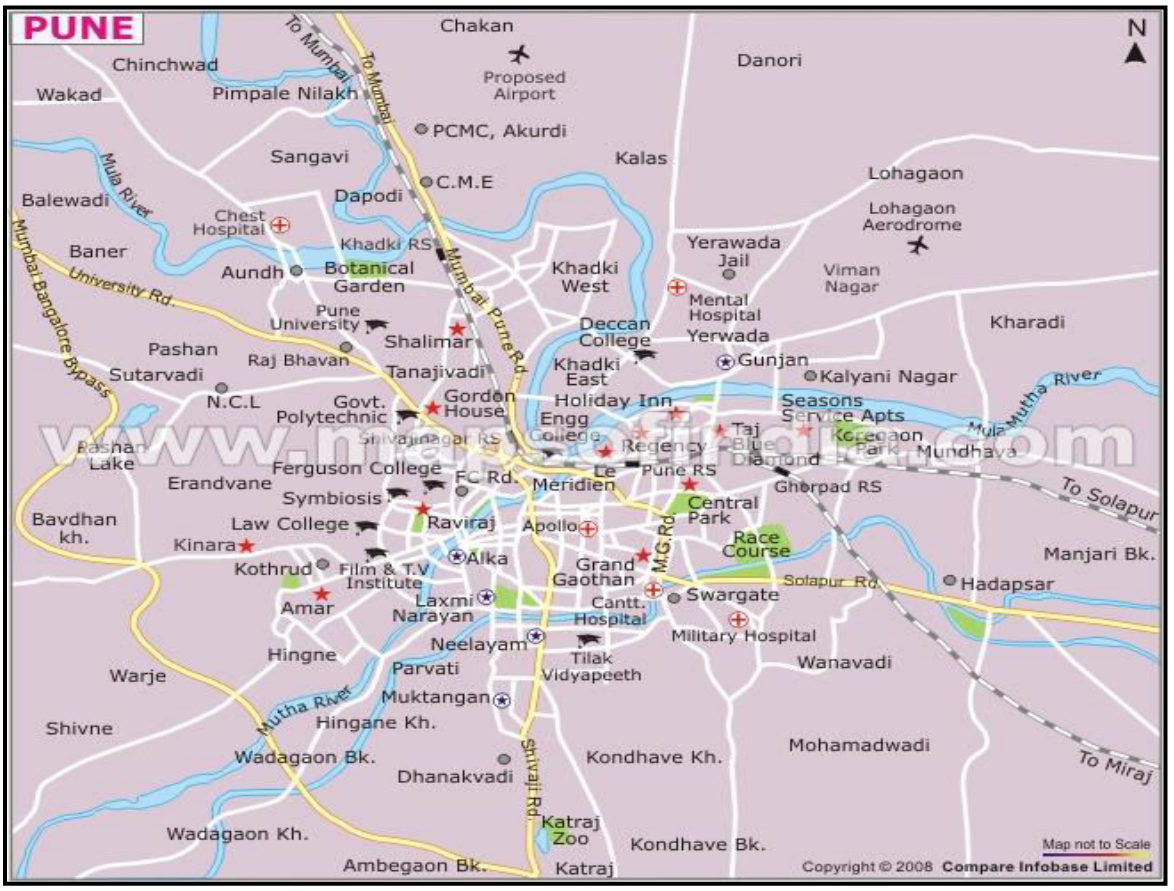
Q.14.As per your point of view, what could be the reason behind the popularity of particular antivirus?

Sr. No	Antivirus Tools	Kaspersky	Norton	Avg	Mcafee	Qhickheal	Netprotector
1	Low cost						
2	Best Performance						
3	Best Service						

Q.15. Please give your comments in 2 -3 lines about your overall experience about Anti-virus Tools. **[OPTIONAL]**

Annexure 3

The geographical location (Maps of India) of the Pune city is indicated by the map 2s.1 as follows



(Source: http://www.mapsofindia.com/maps/maharashtra/pune.htm(23/08/2012)

Map of Pune city

Annexure 4

Publication by Researcher based on this thesis

International Journal Papers

- " A comparative study of selected security tools for personal computer " in International Journal of Computer Application and management, ISSN – 2231-0967, Edition Jan 2012 – VOL III , 9.1 to 9.8

International Conference Papers

- "Management of antivirus tool and security awareness is utmost important for safe usage of personal computer" at the international conference on "Swarajya is my birthright and I shall have it" held at Tilak Maharashtra Vidyapeeth, Pune, during 6th and 7th March 2017.
- " Commercial antivirus tools for personal computers " in international conference INCON VII 2012 (ongoing research in management and IT) held at ASM campus, Pimpri on 3/2/2012 & 4/3/2012, ISBN 978-81-921445-1-1

National Conference Papers

- "Comparative study of commercial antivirus tools for personal computers " in RTIT 2012', the national level conference on 'Recent trends in information Technology' held at JSPM NTC.

National Seminar Papers

- Presented paper entitled "Personal computer Security Policy in the era of Globalization" at national seminar on "Impact of globalization on start- up companies organized by management department of Tilak Maharashtra Vidyapeeth, during 15th March 2015

Annexure 5

Krejcie Morgan's table for sample size determination of a known population

Table for Determining Sample Size of a Known Population

N	S	N	S	N	S	N	S	N	S
10	10	100	80	280	162	800	260	2800	338
15	14	110	86	290	165	850	265	3000	341
20	19	120	92	300	169	900	269	3500	346
25	24	130	97	320	175	950	274	4000	351
30	28	140	103	340	181	1000	278	4500	354
35	32	150	108	360	186	1100	285	5000	357
40	36	160	113	380	191	1200	291	6000	361
45	40	170	118	400	196	1300	297	7000	364
50	44	180	123	420	201	1400	302	8000	367
55	48	190	127	440	205	1500	306	9000	368
60	52	200	132	460	210	1600	310	10000	370
65	56	210	136	480	214	1700	313	15000	375
70	59	220	140	500	217	1800	317	20000	377
75	63	230	144	550	226	1900	320	30000	379
80	66	240	148	600	234	2000	322	40000	380
85	70	250	152	650	242	2200	327	50000	381
90	73	260	155	700	248	2400	331	75000	382
95	76	270	159	750	254	2600	335	1000000	384

Note: N is Population Size; S is Sample Size *Source: Krejcie & Morgan, 1970*

Note:

There is no need of using sample size determination formula for 'known' population since the table has all the provisions one requires to arrive at the required sample size. For a population which is equal to or greater than 1,000,000, the required sample size is 384

Make your facebook account hackproof using following settings continued…

Go in profile →Settings → Security and Login

- Choose friends to contact if you get locked out
- Where you are logged in

  (It will show you all your login details and if you observe any unrecognized logged in, you can log out)
- Login
  - Change password

    (It's good idea to use strong password mixture of uppercase, lowercase, special characters and symbols which is difficult to guess)
  - Log in with profile picture

    (Tap or click your profile picture instead of using password)
- Setting up extra security
  - Get alert about unrecognized logins

    (set this ON)
  - Use two factor authentication

    (Log in with code from your phone as well as password)
- Advanced
  - Encrypted notification

    (Adds extra security to notification emails from facebook so that only you can encrypt those emails)

Make your facebook account hackproof using following settings

Go in profile →Settings → Privacy

- Who can see my stuff
  - Who can see your future post?

    (You can manage the privacy of things you share using the audience. Options are public, friends, friends except, specific friends, only me, custom. Don't set it as public)
  - Who can see your friends list?
  - Review all your posts and things you are tagged in
  - Limit the audience of posts you've shared with friends of friends or public
- Who can contact me?
  - Who can send you friend requests?

    (Options are friends of friends and everyone)
- Who can look me up?
  - Who can look up using email address you provided?

    (Options are friends of friends, friends and everyone)
  - Who can look up using phone number you provided?

    (Options are friends of friends, friends and everyone)
  - Do you want search engines outside of facebook to link to your profile?

    (Set it as No to protect you from identity theft)
- Sensitive Content
  - Cover photos and videos you may not want to see with warnings
    - Partial nudity or sexually suggestive content

(Using above settings you can control your privacy on facebook)

Annexure 7

Browser Security Settings for Google Chrome, Mozilla Firefox and Microsoft Internet Explorer

Tightening your browser's settings is a critical step in using Internet safely and privately. Today's popular browsers include in-built security features but most of the user's often fail to optimize their browser's security settings on installation. Due to which your PC can be put at higher risk for malware infections and cyber attacks. If every PC user follow following tips then it will greatly increase the security of your web browser.

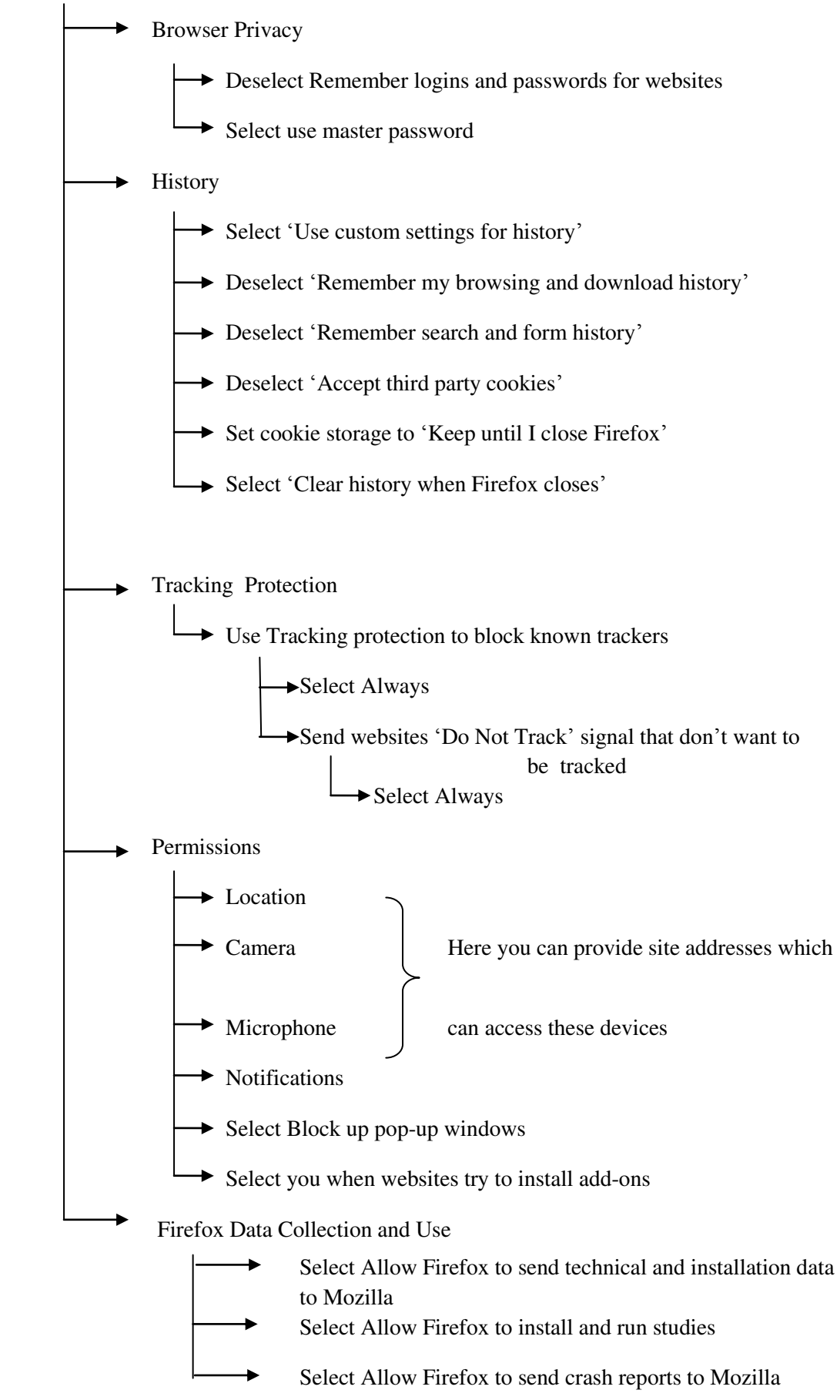
While collecting data it is observed that most of the users use Google chrome, Mozilla Firefox or Internet Explorer as a browser. Hence how to set the privacy and safety settings in it is mentioned below one by one.

Go in Google Chrome →Settings → Advanced → Privacy and Security

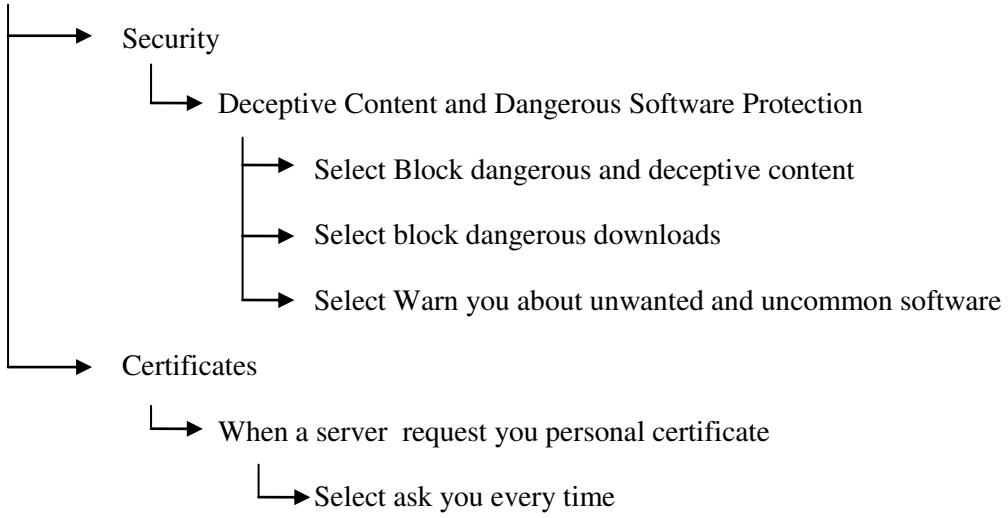
- Automatically send some system information and page content to Google to help to detect dangerous apps and sites
- Protect you and your device from dangerous sites
- Send 'Do not track' request with your browsing traffic
- Manage certificates
- Content settings
  - Cookies
    - Blocked
    - Keep local data only until you quit browser
    - Block third party cookies
  - Location
    - Ask before accessing
  - Camera
    - Ask before accessing
  - Javascript
    - Blocked
  - Flash
    - Ask First
  - Images
    - Do not show any images
  - Popups
    - Blocked
  - Background sync
    - Do not allow recently closed sites to finish sending and receiving data
  - Automatic downloads
    - Do not allow any site to download multiple files automatically
  - Unsanboxed plugin access
    - Ask when site wants to use plugin to access your computer

Google chrome settings

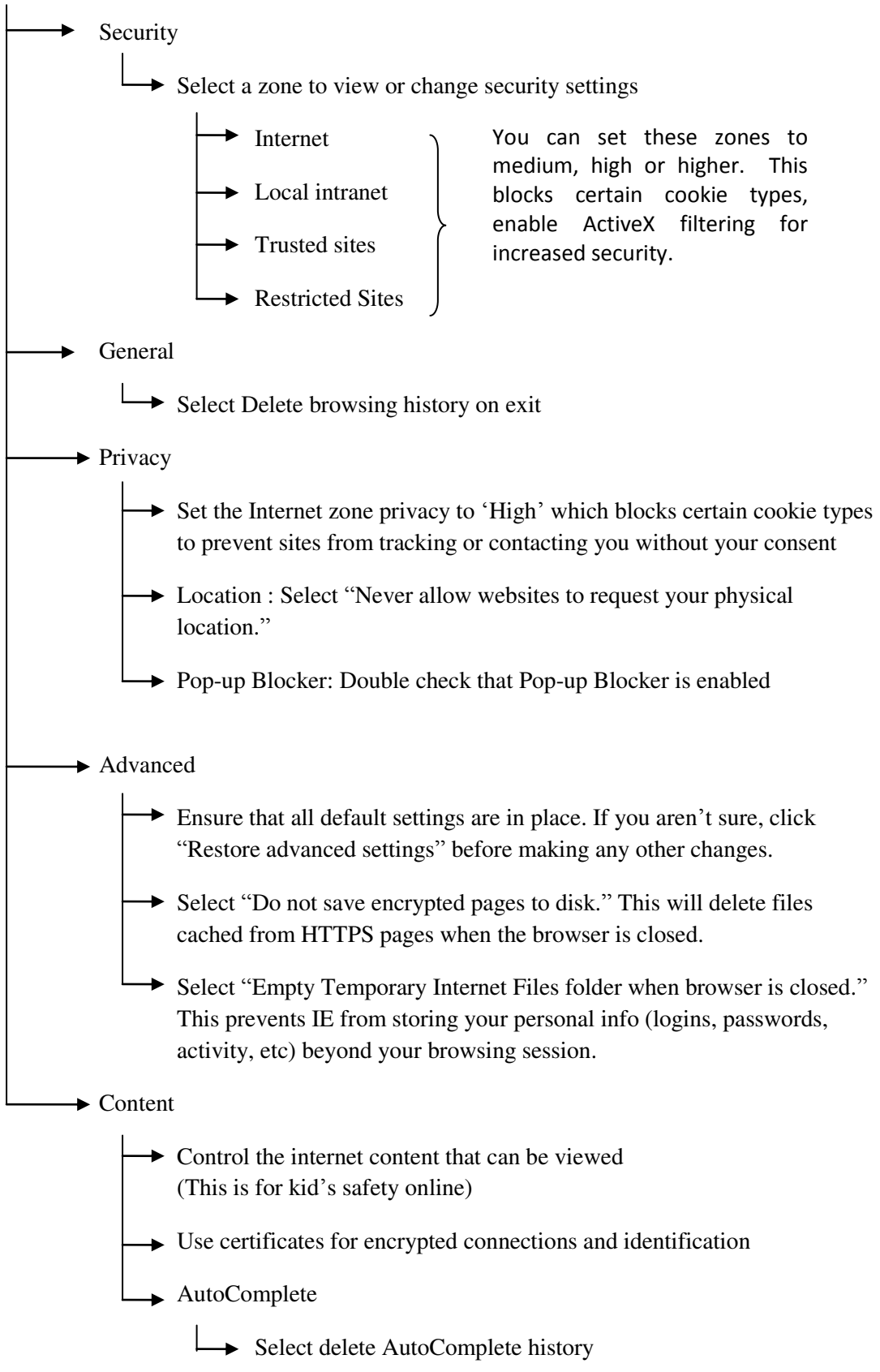
Go in Mozilla Firefox →Options → Privacy and Security



Go in Mozilla Firefox →Options → Privacy and Security



Go in Internet Explorer →Tools Menu → Internet Options



Annexure 8

Securing your mail accounts

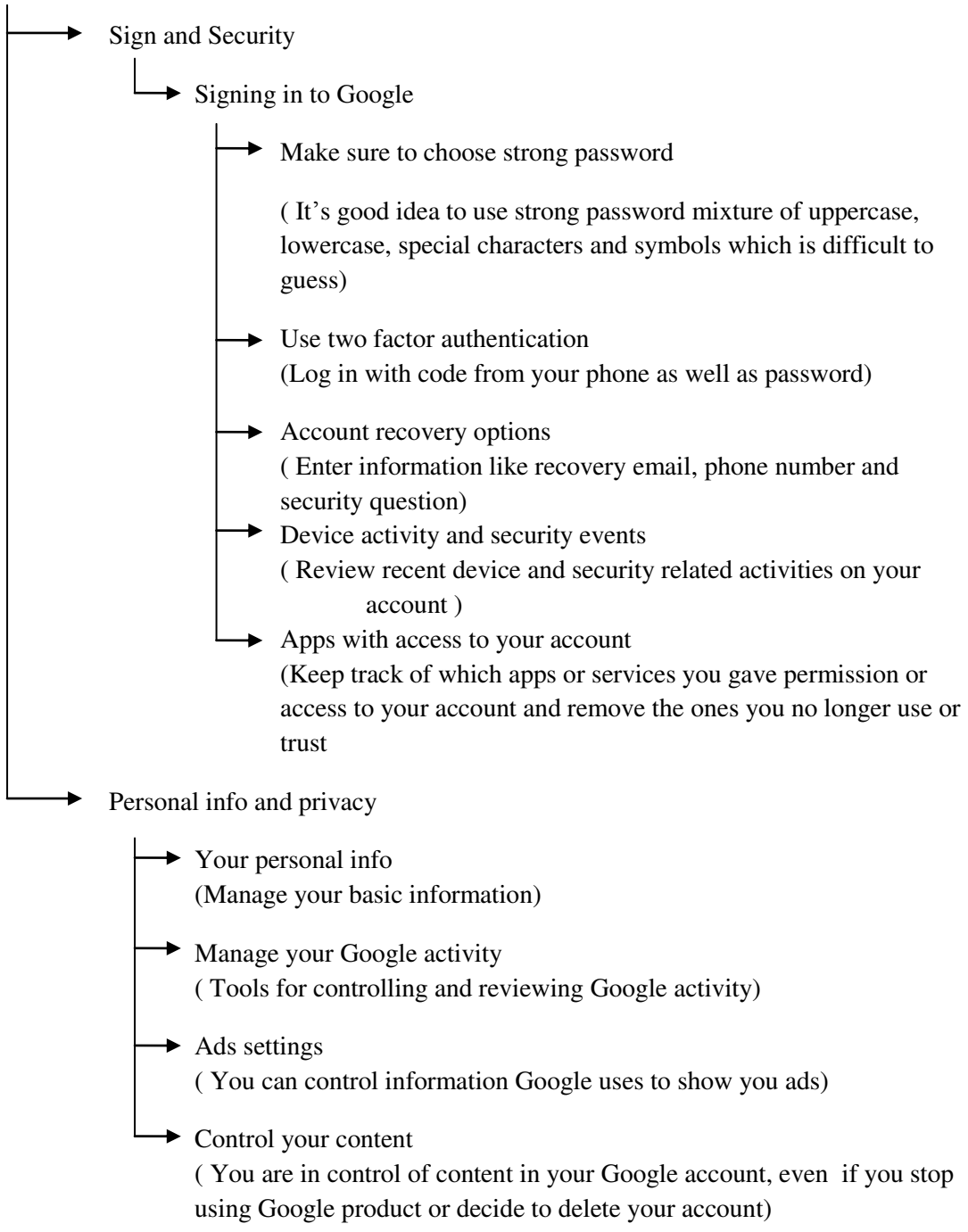
In this information technology era, everyone uses electronic mail as major communication medium. Most of the users use Gmail or Yahoo account for digital communication.

Everybody's mail account may contain sensitive information like

- ✓ Banking Information
- ✓ Account Numbers
- ✓ Salary Slips
- ✓ Personal Information
- ✓ Photographs
- ✓ Private Messages
- ✓ Professional Information etc.
- ✓ Passwords of various accounts

All the information on this platform is at risk with hacked email account. Hence it is very important to secure email account.

Go in Gmail →My Account



Bibliography

- **Books**

1. Brian Bagnall, Ryan Russell, (2000), E-Mail Virus Protection Handbook
2. Crosman , PennyWhich Antivirus software works Best? Testing Lab Reveals Results , American Banker, Vol 178
3. Greenberg, Pam Zombies, Trojan Horses and you, State Legislatures, Vol. 37, 5 May 2011
4. Dr. S. P. Gupta, "Statistical Methods", Sultanchand & sons Publication, New Delhi.
5. Dr.Fedrick B. Cohen, " Short course on computer viruses", second Edition, Willey Professional computing
6. Eric Filiol , (2005), Springer, Computer viruses: from theory to applications
7. Joxean Koret, Elias Bachaalany, The Antivirus Hacker's Handbook, ISBN:978-1-119-02875
8. John Aycock, "Computer viruses and malware", Springer
9. C.R.Kothari, "Research Methodology Methods & Techniques", New age International Publication, New Delhi.
10. Karsten Johansson, (1994), COMPUTER VIRUSES: The Technology and Evolution of an Artificial Life Form
11. Matt Smith , HackerProof: Your Guide to PC Security
12. Michael Sikorski and Andrew Honig, "Practical Malware Analysis : A Hands On guide to Dessecting Malicious software, no Starch Press, San Francisco
13. Michael Erbschole, , (2005), TROJANS, WORMS, AND SPYWARE A Computer Security Professional's Guide to Malicious Code
14. Mark Ludwig, "The giant book of Computer viruses", Lulu.com, 2016, ISBN 136551093X, 9781365510939
15. Mark Ludwig, "The little book of Computer viruses"
16. Peter Szor, The Art of Computer Virus Research and Defense. Addison Wesley Professional, 1 edition, February 2005
17. Rune Skardhamar, Virus detection and Elimination, AP Professional,1996
18. Sophos, (2004),Viruses and spam

19. Ms. Nandita. G, Computer virus

20. Snorre Fagerland, Sylvia Moon, Kenneth Walls, Carl Bretteville , (2001) , The Norman Book on Computer Viruses

- **Journal and Magazines**

1. Ahmad, D. W. (2010). Computer Viruses as a Threat to Home Users. International Journal of Elecrical & Computer Sciences IJECS , 29-34.
2. Bhaskar Patil, a. R. (2014). Computer Virus and Antivirus Software –A Brief Review. International Journal of Advances in Management and Economics,ISSN: 2278-3369 .
3. Dillon, R. (2007). A simple guide to Computer Viruses and other dangerous little programs - An Introduction to an effective defense. International journal of law and technology, Program and Play -
4. Erbschloe, M. (2005). TROJANS, WORMS, AND SPYWARE A Computer Security Professional‘s Guide to Malicious Code.
5. Gregory, P. (2004). Computer Viruses for Dummies. Wiley,ISBN: 0-7645-7418-3.
6. H. Shravan Kumar & Prof. Bernard Menezes. Study of Viruses and Worms. KReSIT, I.I.T. Bombay.
7. Hauge, C. (2006). Anatomy of Computer Viruses. CPH Solutions .
8. Jeffrey O. Kephart, G. B. (1998). Biologically Inspired Defenses Against Computer Viruses. High Integrity Computing Laboratory .
9. Johnson, S. R. (2000). Computer Virus – Technol ogy Tips. IOWA State University, PM 1789.
10. Li, X. (2003). Computer Viruses: The Threat Today and the expected future. Information Theory Division, Linköping Institute of Technology,LiTH-ISY-EX-3452-2003 .
11. Marshall, D. J. (1999). Computer Crimes: How to avoid falling Victim. Journal of Industrial Technology .
12. Miller, L. C. Cybersecurity for Dummies, A Wiley Brand. A Wiley Brand, Palo Alto Networks 2nd edition, CISSP.
13. Mok, R. H. (2004). Detecting Unknown Massive Mailing Viruses Using Proactive Methods. UTCS Technical Report RTS-TR-04-0 .
14. Mr. Bhaskar Patil, D. M. (2010). A Comparative Study for Performance Measurement

of Selected Security Tools. International Journal of Engineering Science and Technology Vol. 2(10), 2010, , 5130-5136.

15. Olivier, M. (1990). Computer Viruses:. Centre for Advanced Computing and Decision Support CSIR , 1-12.
16. Orathai Sukwong, H. S. (2011). Commercial antivirus software effectiveness : An empirical study. IEEE Computer Society .
17. Paul Royal, M. H. PolyUnpack: Automating the Hidden-Code Extraction of Unpack-. 22th Annual Computer Security Applications Conference (ACSAC 2006). Miami Beach, FL: 2006.
18. PC Magazine. (n.d.). Retrieved 1 2, 2014, from PC Magazine: www.pcmag.com
19. Pele Li, M. S. (2008). A Survey Of Internetworm Detection And Containment. Ieee Communications, The Electronic Magazine Of Original Peer-Reviewed Survey Articles, 1st Quarter , 10.
20. Peter Mell, K. K. (2005). Guide to Malware Incident Prevention and Handling . National Instotute of Standards and Technology, U.S. Department of Commerce , 800-83.
21. Protecting Your Computer and Your Identity, Security Awareness, Office of Enterprise Security. (2007)
22. Rizwan Rehman, D. G. (2011). Malware Threats and Mitigation Strategies: A Survey. Journal of Theoretical and Applied Information Technology .
23. Shuhaili Talib, N. L. (n.d.). An Analysis of Information Security Awareness within Home and Work Environments. Centre for Security, Communications and Network Research (CSCAN),University of Plymouth, Plymouth, PL4 8AA,United Kingdom .
24. Wielputz, R. (2007). Evolution! From Creeper to Storm, Seminar on Malware. Bonn-Aachen International Center for Information Technology .
25. XieHong, S. &. (2010). Computer Virus Preventing and Controlling Method Discussion. Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops (ISECS '10).

- **Reports**

1. Av test security report 2015/16. av-test
2. Antivirus Comparative. Summary report 2016
3. Antivirus Comparative. Summary report 2016

4. IT Security Survey 2016 on Antivirus .
5. Marko Helenus, "A System to support the analysis of antivirus product and virus detection capabilities", Karen Mercedes Goertzel, Theodore Winograd, (2009) Information Assurance ,Tools Report – Malware,2002
6. Stanley R. Johnson, Computer Virus - Technology Tips, IOWA State University,PM 1789j Revised, June 2000
7. Tim Rains, Director of Trustworthy Computing at Microsoft. (2013, 04 17). Latest Security Intelligence Report Shows 24 Percent of PCs are Unprotected.

- **News Papers**

1. Daily News Analysis (DNA), LifeStyle Report - CyberBullyng Social Media Darker Side
2. India Today – P.M Narendra Modi Address Nation
3. End cyber Bullying – India Ranks 3rd in Cyber Bullying

- **Theses**

1. Rainer Link, Prof. Hannelore Frank, Prof. Dr. Rainer Mueller, (2003) Server-based Virus-protection On Unix/Linux
2. Matthew PaulWebster, (2008), "Formal Models of Reproduction: from Computer Viruses to Artificial Life"
3. Xin Li, Viiveke Fåk,(2003), "Computer Viruses: The Threat Today and The Expected Future"
4. Roberto Dillon, (2007), "A simple guide to Computer Viruses and other dangerous little programs - An Introduction to an Effective Defense"
5. Marko Helenius, Pretti JarvInen, (2002), "A System to Support the Analysis of Anti-virus Products' Virus Detection Capabilities"
6. Markus Fors, Christian Grahn, Stefan Alfredsson, (2010), "An implementation of a DNS-based malware detection system"
7. Daniel J. Cross, Luiz Felipe Perrone, (2005), "An Investigation into the Human/Computer Interface from a Security Perspective"
8. Fausi Qattan & Fredrik Thernelius, (2004), "Deficiencies in Current Software Protection Mechanisms and Alternatives for Securing Computer Integrity"

9. Ali Ikinci, Prof. Dr.-Ing. Felix C. Freiling, Prof. Dr.-Ing. Wolfgang E_elsberg, (2007), "Monkey-Spider: Detecting Malicious Web Sites"
10. Raghunathan Srinivasan, (2007), "Protecting Anti-Virus Software Under Viral Attacks"
11. Johan Sandin, (2005), "An Overview of Malware Protection Approaches on Client Computers"
12. Najib Bin Limun, (2005), "The Use Of Intrusion Prevention System To Increase Computer Security"
13. Bhaskar Vijay Patil , "A study of performance evaluation of antivirus software in Kolhapur and sangali district" , Under the faculty of commerce, Shivaji University, Kolhapur

- **Websites**

1. Antivirus Comparative. Summary report 2016. www.av-comparatives.org.
2. Av Comparatives. (n.d.). Retrieved 8 6, 2016, from Independent Tests of Anti-virus Software: https://www.av-comparatives.org/
3. Av Test Independent It Security Institute. (n.d.). Retrieved 4 2, 2014, from Av Test Independent It Security Institute: https://www.av-test.org
4. AVG Antivirus. (n.d.). Retrieved 10 18, 2013, from World class protection: www.avg.com
5. av-test.org. (2016). Av test security report 2015/16. av-test.
6. Bishop, M. (2011). An Overview of Computer Viruses in a Research Environment. Computer Science Research Symposium (CSRS2011) .
7. Browser Sandbox. (n.d.). Retrieved 3 3, 2016, from What is browser sandbox protection and how does it help: http://www.slideshare.net/QuickHealPPTs/how-much-should-you-reveal-on-social-media?from_action=save
8. Cohen, F. (1987). Computer Virus: Theory and Experiment. Computer & security 6 , 22-35.
9. Computer viruses and what they mean to you. (n.d.). Retrieved Jan 25, 2015, from www.quickheal.co.in: http://www.quickheal.co.in/resources/articles/computer_viruses_and_what_they_mean_to_you#sthash.cpx7BJmc.dpuf
10. Fenlon, M. B. (2010). How Computer Viruses Work. Retrieved 3 30, 2016, from HowStuffWorks: http://computer.howstuffworks.com/virus.htm

11. http://en.wikipedia.org/wiki/Pune(11/7/2016)
12. http://government.wikia.com/wiki/PMC_Electoral_Ward_Administration (20/6/2009)
13. http://searchmidmarketsecurity.techtarget.com/definition/keylogger
14. http://searchsecurity.techtarget.com/definition/attack-vector
15. http://searchsecurity.techtarget.com/definition/back-door
16. http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques
17. http://www.census2011.co.in(1/1/2012)
18. http://www.maharashtrafireservices.org/pdf/pune_mitigation_plan.pdf (23/09/2016)
19. http://www.mapsofindia.com/maps/maharashtra/pune.htm(23/07/2016)
20. http://www.techrepublic.com/blog/10-things/10-ways-to-avoid-viruses-and-spyware/
21. http://www.webopedia.com/TERM/P/phishing.html
22. https://antivirus.comodo.com/blog/computer-safety/5-imple-steps-protect-pc/
23. https://www.howtogeek.com/228828/7-ways-to-secure-your-web-browser-against-attacks/
24. https://www.techopedia.com/definition/1678/virus-hoax
25. https://www.techopedia.com/definition/39/blended-threat
26. https://www.veracode.com/security/rootkit
27. India ranks 3rd in cyber Bullying. (n.d.). Retrieved 11 3, 2016, from http://www.endcyberbullying.org: http://www.endcyberbullying.org/india-ranks-third-on-global-cyber-bullying-list/
28. India Today. (2016, 11 08). Retrieved 01 15, 2017, from http://indiatoday.intoday.in: http://indiatoday.intoday.in/story/live-pm-narendra-modi-addresses-nation/1/805755.html
29. Kaspersky Lab. (n.d.). Retrieved 10 15, 2016, from The power to protect what matters most: https://www.kaspersky.co.in/
30. Mcafee Antivirus. (n.d.). Retrieved 6 3, 2016, from Find your security solution: https://www.mcafee.com
31. Net Protector Total Security. (n.d.). Retrieved 7 7, 2016, from http://www.indiaantivirus.com
32. Norton Antivirus. (n.d.). Retrieved 6 6, 2016, from 100% Virus protection promise: https://in.norton.com
33. Norton By Symantic. (n.d.). Retrieved 4 4, 2016, from Password Pains: https://in.norton.com/password-pain/article
34. Quick Heal Antivirus. (n.d.). Retrieved 10 15, 2014, from Security Simplified:

http://www.quickheal.co.in/

35. side, C. S. (2012, 07 08). Retrieved 03 11, 2015, from dnaindia.com: http://www.dnaindia.com/lifestyle/report_cyberbullying-social-media-s-darker-side_1712080
36. slideshare . (n.d.). Retrieved 2 2, 2016, from How much should reveal on social media: http://www.slideshare.net/QuickHealPPTs/how-much-should-you-reveal-on-social-media?from_action=save
37. TechLineInfo. (2013, 10 13). Retrieved 5 20, 2014, from A Brief History of Antivirus Software, techlineinfo.com: http://www.techlineinfo.com/a-brief-history-of-antivirus-software/
38. Tim Rains, Director of Trustworthy Computing at Microsoft. (2013, 04 17). Latest Security Intelligence Report Shows 24 Percent of PCs are Unprotected. Retrieved 07 21, 2015, from https://blogs.microsoft.com/blog/2013/04/17: https://blogs.microsoft.com/blog/2013/04/17/latest-security-intelligence-report-shows-24-percent-of-pcs-are-unprotected/#Y7FCKDZ0QtrOIlXs.99
39. Virus Bulletin. (n.d.). Retrieved 10 18, 2014, from Covering the global threat lanscape: https://www.virusbulletin.com/
40. What is VPN?Your key to online privacy. (n.d.). Retrieved 1 1, 2016, from AVG Antivirus: http://www.avg.com/us-en/hma-pro-vpn
41. Wikipedia. (n.d.). Retrieved 08 21, 2013, from Pune: http://en.wikipedia.org/wiki/Pune