How do viruses function on the internet and how can they be prevented?

Over the last few years, computer viruses have evolved enormously and people responsible for creating such viruses have developed novel methods to penetrate through computer security measures. In general, computer viruses refer to the programs that intentionally or unintentionally gain access to individual computers or a computer network and disrupt the overall functioning of the system; in turn, viruses may or may not cause damage to computer data or installed programs. Viruses have been around since the 1980s and according to research conducted by Subramanya & Lakshminarasimhan (2001), there are more than 40,000 different types of viruses . Even though viruses effect computers systems and internet service in the aforementioned way, a safer environment for internet users can be achieved though security software and users awareness and .In the following essay, I will discuss that viruses function by violating personal privacy and damaging computer files and functions. In understanding the function of viruses in this manner, I further contend the prevention of internet viruses is best achieved by comprehensive security measures alongside public education and user awareness.

Firstly, viruses on the internet can violate personal privacy and access the secret information for individuals and organizations. Moreover, among this types of viruses that are present on Internet, spyware and adware are the two most common viruses. The functionality of Spyware is to get the information of users without their consent and then use it, store it or sell this information to third parties for various purposes such as stealing, advertising , marketing objects (Lavesson, Boldt, Davidsson, & Jacobsson, 2011). Spyware has a significant impact over the last few years mainly because of the increase in the marketing and advertising industry and can be categorised as 'mild or wild'(Ames, 2004). The exact information viruses collect may vary due to various aspects, however it mostly contains things that have value such as collecting information about users **identity document** , Password, email addresses and lists which is the most targeted by spammers, software license keys, visited websites and other important information. Even though Adware *is also a way in which viruses* violate users privacy and similar to spyware in the process of collecting data and storing the information of the users over the Internet but different purpose do exist. Also, it is focusing more on marketing and used customarily by marketing or advertising companies to target people with specific search criteria(Erbschloe, 2005).Symptoms of Adware are popup advertisements on one's computer screen, or unwanted banners on browsers.

In addition, to Getting access to individuals and orgnaisations privacy . Other function of viruses such as Trojans and worms are disrupting systems and networks. Trojans and worms They are problematic for its harmful effects and at the same time are considered as the basic type of malicious code designed primarily to give hackers access to system files for various purposes, such as monitoring the activity of user and stealing important information like users identifications and passwords. The main purpose of Trojans is to damage computer files (Erbschloe, 2005). There are various types of Trojans, that are usually classified based on the actions they perform on your computer. In reference to worms, they can be classified as virus by design and are usually considered to be a sub-class of viruses. A worm is usually classified as a computer program that spreads without the interaction of the user. Worms usually spread from one computer to another one, unlike other viruses. One of the biggest harms that a worm carries, is its capability to replicate itself on a system so rather than a computer sending out a single worm, it usually send out copies of itself in large quantities, creating a huge devastating effect (Erbschloe, 2005). Due to the constant threat of worms to the infrastructure of the network, it has become one of the most important and highly critical matters for network equipment designers (Oorschot, Jean-Marc, & Miguel, 2006).

Every time there is a new threat to computers, having comprehensive anti-virus policies is an effective method that can be used or adopted in order to avoid such risks or threats. Some of the most common comprehensive ways to avoid such virus related threats is the "protect all entryways" solution. This solution ensures inclusive protection through the installation of antivirus software and the scanning of the three modes of data transfer; that is to say, the scanning of the storage servers, the internet gateways servers or network servers, and the end user's devices. There are, however, a number of drawbacks to such a solution. These drawbacks can include a slowing down of a user's operating system as well as the need to continually update the anti-virus software. Even when considering these drawbacks, however, it is evident that comprehensive policies such as the 'protect all entryways' solution is an effective method in achieving immunity against viruses and maintaining virus-free networks. Therefore, the "protect all entryways' solution plays a significant role in protecting computers against all types of viruses, whether it be spyware, adware, trojan, worms or other types of computer or network viruses (Monds, & Wang, 2003). There are, though, it must be acknowledged, other threats which this solution is unable to address. These other threats arise out of human mistakes and a lack of awareness, for instance, downloaded information from untrusted sources; email viruses; and a user accepting any terms from unknown websites or non-authorized service providers.

The other important factor for individuals, governments and organizations in preventing internet virus threats and enhancing safe internet environments is through the improvement of user awareness regarding security measures and how to avoid virus attacks (Kruck & Teer, 2008). User education seems to be the most effective way of avoiding potential threats and other risks that may be imposed on internet users (Hawkins, Yen, & Chou, 2000). This strategy informs the user of the source of viruses and enables the user to appropriately respond to virus threats and security issues. As well as this, this strategy also provides users with the knowledge of the importance of security measures which in turn encourages users to act more responsibly in regards to their internet activity (Wen, 1998).

FROM THE EVIDENCE I HAVE OUTLINED/DISCUSSED, IT IS THEREFORE CLEAR THAT WE SHOULD ADOPT THIS PREVENTION METHOD

It is for these important reasons to educate, end users, first level support staff or even people in management positions to ensure they make the necessary decisions if any virus attacks them.

Over the years the overall industry of the Internet has evolved as one of the most important parts of individual life. Almost every single detail of a person is available on Internet, his photos, banking details, email passwords, legal documents so on and so forth. Many people like to get access to such information for various purposes, some do it for fun and some for professional reasons. In order to get such information or to harm other computers, different types of viruses have been developed. Some of the most common viruses are Trojans, Spyware, Adware, and Worms . The functions and purposes of every virus is different To be secured from these viruses there are various antivirus programs developed by companies, but such antiviruses alone are not enough for security purposes. Along with the ant-viruses, it is important that users are well aware of such viruses and in case if they experience any irregular or suspicious activities on their system they should know what necessary steps they can take. In creating such awareness, government and other Internet service providers have a major and important role to play, through which they can ensure individuals have realized that such education could help them to secure devices and data.