Email security essay

It is a paradox that in spite of the advances in technology that we are witnessing today one's privacy and security of data in the internet is often compromised to a very large extent. Often, personal information of individuals is stolen or financial data of companies are whisked away by elements who could put this information to the wrong use.

It is in this scenario that privacy of data has become an important issue for computer users all over the world. Privacy of data becomes more important when one works in a public domain like the Internet. This paper will suggest some of the precautions that an ordinary person needs to take to maintain personal privacy and ensure safety of data while working with emails. Analysis The advent of the internet has changed the way in which technology was being used to support businesses as well as personal needs of users worldwide. Little did people realize that the internet would establish itself as a powerful facilitator of the needs of the common man in such a short period of time. However the same facilities that the Internet offers can also be a potential source for dissemination of our private information without us even knowing about it.

Email security threats may be of many different types. Email security can be compromised by spoofing, identity theft, attacks by modifying existing messages, and imposters [Kangas, 2004]. Hackers may use any or all of these methods to break into a user's computer. Email security Email is one of the most potent sources for losing our data because most people are complacent about enforcing email security. Email software is also the most used software among computer users. Hence, any vulnerability of popular

email software can be easily exploited by unscrupulous elements to gain entry into the private data of a lot of people.

Hence, it is very important that every one use secure email clients for receiving and sending emails. A lot of reputed email clients are available and the company that makes them releases security patches from time to time. All these patches from the company must be installed to plug any software vulnerabilities. It must be understood that the computer architecture that is used to exchange emails are not very secure and does not provide for much privacy for the users.

On the other hand, software like ‘ sniffers’ is available in the market, which can effectively capture data that is meant for some other computer. Hence, the need for encrypting data is very important. Encryption techniques ensure that messages meant for a person can be read by that person alone. A very well known email encryption is PGP (Pretty Good Privacy) that is free and secures [Engelfriet, 1998]. An easy way for computer hackers to steal information is by using viruses and Trojans, which are computer programs that perform undesired actions on one’s computer without one’s knowledge. Hence, all emails must be scanned with good anti-virus software.

Similarly, emails from entrusted sources must not be opened and have to be checked for viruses before they are opened [GFI, 2004; Slavic, 2004]. Privacy of email user is compromised by spammers who send unsolicited mails to one’s address. In addition to being a nuisance, spam wastes a lot of email server space thereby jeopardizing the receipt of important mails. In addition, spam may also contain viruses and Trojans that could seriously harm one’s

computer. It is very essential to keep one's email id private in order to avoid spam. It is always advisable to keep alternate email addresses that may be used when email ids have to be given for website registrations.

Hackers have been known to use the names in the address line of personal email ids to crack email passwords. By keeping your email private, and publishing only an alternate email id that can be discarded at will, users can avoid being tracked by cookies, prevent spammers, and also prevent easy access for hackers. It is advisable to install and use personal firewall software in order to prevent security threats and also to protect the identity of the user's machine on the Internet. When a user logs on to the Internet, sites will be able to identify the user's IP address, which could help hackers to break into the user's computer. A firewall provides an additional level of security to the user so that his personal details are hidden from hackers on the net