Operating system of the computer

Technology, Computer

This is a software which, when installed in the operating system of the computer, will be able to record information on the activity of the person using the computer. It is a type of spyware when it is written by criminals who want to take control and steal information from the computer user. The software may gain entry to the computer and installed secretly when an email attachment containing the spyware in the form of virus or “ trojan” is opened, or when a link to the software is clicked while visiting a website.

It can also be installed using a USB key when the criminal has physical access to the computer, even though when the computer is unattended for a few minutes. Information concerning the computer activity such as keystrokes entered, website history, emails sent or received, chat logs etc. can be logged and sent remotely to the criminal through the Internet. The criminal may then be able to extract personal information such as bank account numbers, credit card numbers, login IDs and passwords etc. and use the information for stealing money through Internet banking.

At times, the software may be installed by the owners in their computers deliberately. One less common use is as a recovery tool. If there is accidental data loss, one can use the keystroke records to recover what was typed. Very often, the software is used without the knowledge of the one being monitored. Parents use the software to keep track of their children’s Internet access, filter content, block websites and log chat conversations. Managers might want to monitor the computer activities of their employees with the purpose of analyzing working habits and keep track of computer usage for security. However, companies may be sued for the use of keystroke logging software without the knowledge of the employees.

Nowadays, one only has to search on the Internet to find that there are many commercial keystroke logging softwares available at a cheap price. Companies selling these kind of software have emphasized that no advanced computer knowledge is required to use it. Anyone with adequate computer knowledge can install a keylogger on your computer without your knowing that your activity is being watched from that day onwards. A good keylogger leaves no trace after it's installed; you won't even notice that it's there! No apparent change is noticeable in system performance. Everything looks normal. And before you know it, your account password has been changed and someone else is making a purchase with your credit card data!

As you can see, our privacy in the use of computers and the Internet is not guaranteed. In the past, only a few people with a certain level of computer knowledge were able to monitor their targets' computer activity. It is quite overwhelming to think that even your parents, your classmates, your boss or your colleagues can easily track what you are doing. Certainly, we must make personal communications throughout the day, whether it is e-mail or Instant Messenger, just as a normal course of our daily lives, sending an email to a friend, or chatting to a classmate about homework, and this particular software would pick up those conversations as well. Are we not allowed to have a life of our own? Must our every action on the Internet be monitored? How could we have freedom of speech but not privacy on the Internet? It's certainly ruthless in its pursuit.

But what about when parents use it as a monitoring tool on their children? Parents might think that this is only a harmless but effective way to ensure

children’s safety on the Internet, especially when the kids are young and vulnerable to predators on the net. However, children might think that parents are infringing their privacy. It could even lead to a decline in parent-child relationship once the child realizes that every word he or she types has been recorded and inspected by the parent. Certainly, installing keystroke logging software is not the best way to monitor their children’s computer activity. Instead, parents should educate kids the right attitude when using the Internet, and communicate with their children more often in order to understand them, not just by reading what they type in emails, Facebook posts, or chat conversations.

Moreover, the use of Internet banking and online shopping is becoming more and more commonplace. Dozens of passwords for our various accounts are needed, such as email, Facebook, Instant Messenger, bank accounts, Apple store and Amazon etc. We would suffer great loss when our information is collected easily by others and used for criminal means. In this case, we have to stay alert for the possibility of being spied upon and take necessary precautions. The computer language or code is beyond the comprehension of normal people so that there is no easy way to detect when our computer has a keystroke logging software installed. Personal vigilance, anti-spying software, or constant improvement in the computer hardware or software technology may help to patch up any loopholes discovered by computer hackers.

3. The inference of the Government on the information that its citizens get The Internet is a place we all go to, like any mall or plaza. There, we can

express our opinions freely and have access to information that we need. However, interference of the government on the information that its citizens get is also seen in different countries. Some countries have state-mandated filtering. For example, in Africa, the Middle East and Central Asia, the Internet is highly under persuasive censorship and the surfers have a limited access to the Internet.

China is a prime example. It has marked itself out and highly censors and represses the use of the Internet and access to information about sensitive topics in China. When the Internet user requests for a banned website that contains content that the Chinese government disapproves of, a false ‘ time-out’ error indication without any explanation appears on the screen and further prevents the user from going to other banned websites. This shows that the Chinese government is highly concerned about what their people read about them on the Internet. When sensitive keywords are typed in search engines, like ‘ 64’, ‘ jasmine’, ‘ cultural revolution’ etc., the false error indicator pops up.

The Chinese government highly censors the use of Internet because it knows that power is unimaginable, as it is a common platform for everyone from all over the world to communicate and interact and revolutions against the country can be easily started; it does this because of fear. However, people who live in China don’t know what is happening around them as they know of nothing of the news in China; they are living in ignorance and confusion.

Many people in China still don’t know what happened during the 6-4 event, which caused huge international fury and calling to Chinese government to

stop political oppression. We have a right to information that is genuine and accurate, and the people who live in China definitely have a right to know the truth about important events that happened in their own country. In the Universal Declaration of Human Rights, it says that ‘ Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference, and impart information and ideas through any media regardless of frontiers’.

What the Chinese government is doing seizes away the liberty of citizens. Google also accuses China of interfering with their Gmail email system, making it impossible for users to send messages, mark messages as unread and access to other services. It says that human rights activists are the main target of China’s attack to Internet freedom. And China also does it quietly without drawing too much attention, contrasting the Middle East.

This is outrageous. What China does violates the rights of its citizens of freedom and privacy. We all have a password for our email accounts, but the prime use of it is lost if the government can just hack into our accounts and control our movement on the Internet. The International Convenant on Civil and Political Rights of the United Nations in 1966 states that ‘ No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’, protecting the privacy of all people on earth.

4. Web Advertisements Advertisements have been around for a long time. Nowadays in the 21st century, we see advertisements everywhere around us

– even on the Internet. Web advertisements may seem harmless enough, and do not really bother us, but recently, some people are beginning to wonder whether they do infringe our privacy. Ever wondered why whenever you log onto your Gmail account, the advertisements in the ad column correspond to the content of your Gmail? Gmail reads our email and shows us different advertisements that correspond to the content of our emails.

Google has a special software called Googlebots, which reads the texts in your email, then identifies relevant keywords in your email and puts the keywords in a cookie. Semi-related advertisements are then fetched from its inventory. Google assures us that they do not share our personal information with advertisers. Although some may say that this infringes on our privacy, some think that this function benefits their users by recommending useful advertisements to users instead of random advertisements.

The disadvantage is knowing your emails are being read. Watching videos on YouTube is a favorite pastime of a lot of people; we have fun just watching random ones. But when you go back to the homepage after a little while, one would see that they have a section called Recommended Videos, showing various videos. Web advertisements may increase our convenience, but they infringe our privacy by tracking our actions.

Conclusion

Rapid technology advancement in the Internet has brought about huge impacts on our daily life. It has greatly improved our communication with each other and with the rest of the world. Our life has been changed greatly:

with Internet banking, people do not need to waste time queue up for bank transactions; with Internet shopping we not longer need to travel a long way in order to buy something for our home.

However, these advances are not without a price. In the computer and Internet world, it is our privacy that is at stake. In fact the very time when our computer is connected to the Internet, all the data we send or receive has the potential to be intercepted and retrieved by people other than the one we intended to send, as the data has to travel a long way, mixed with data from other people, through cables shared by various servers before reaching its destination. Our Internet Service Provider, through which we connect to the Internet world will temporarily store the data that we send or receive in its server, thus it is prudent to assume that all our communications, like email, are already accessible by our ISP.

We may also leave information about the websites we have visited, the things that we have just purchased when we browse the Internet in form of tracking cookies. These cookies may infringe on our privacy when they are used to track our browsing habits, our preferences for particular items when we do Internet shopping. Google, a major Internet host has gone so far as to read our emails with a specially designed software to identify keywords in our email so as to send out advertisements that we may be interested in reading.

The new craze of social networking websites like Facebook becomes popular platforms where people can chat with their friends and make new ones. However, Facebook also becomes an important area where we may lose our

privacy and personal data. Our identity data such as age, gender and birthday may be exposed to anyone. Also, facial recognition technology, whilst providing convenience for us to tag the photos with the names of our friends, opens a large loophole where people can purposefully get to know everything about us just by seeing our photos on Facebook and clicking our name to read our profile. Moreover, Facebook saves the facial features of people into a database, which might bring undesirable results when fallen into the wrong hands.

The most worrying case is the availability of keystroke logging software which may be installed secretly by other people into the computer without the owner or the user knowing. At times the software is purchased commercially and installed by the owner to monitor children or employee performance. In some counties, the government can just hack into citizen's accounts and control their movement on the Internet. The Internet is highly under censorship and the surfers have a limited access to it.

In our research, we have investigated the functions and uses of different technology, as well as their impact on our privacy. It is apparent that the development of computer and Internet technology, while bringing a lot of improvements to our daily life, also bring about negative impacts on our privacy. We may safe guard our privacy by understanding and avoiding the pitfalls where we may lose our personal information in the web. Hopefully, with more powerful computers, more sophisticated software designs and more stringent data handling required of the Internet service provider

through proper legislation, we may be able to regulate the storage and dissemination of our personal information through the web.