Computer science assignment

Science, Computer Science

Ahmad likes to spend hours and hours playing online games. One day, while he was playing online games, unexpectedly onscreenadvertisementappear on his computer screen. His computer suddenly shut down by itself. When he tried to switch on his computer takes a longer times than normal to start. This scenario relates to computer security risk.

What meant by computer security risk?

According to Gary B. Shelly and Misty E. Vermaat from the Discovering Computer(2012) computer security risk is defined as any event or action that could cause a loss of or damage to computer hardware, software, data, information or processing capability. There are a few types of computer security risk such as Internet and Network attack. It definition is any information transmitted over networks has a higher degree of security risk than information on an organization's premises. Some of example is Malware, Spoofing, Botnets, Back doors and others. Second, unauthorized access and use.

Unauthorized access is the use of computer or network without permission. Unauthorized use is he use of a computer or its data for unapproved or possibly illegal activities. Third, hardware theft and vandalism. Hardware theft is the act of stealing computer equipment meanwhile hardware vandalism is the act of defacing or destroying computer equipment. Besides, software theft also the computer security risk.

Software theft occurs when someone steals software media, intentionally erases programs, illegal copies a program or illegal register a programs. Fifth, information theft occurs when someone steals personal or confidential

information. The last types of computer security risk is systemfailure. System failure is the prolonged malfunction of a computer caused by the aging hardware, natural disasters and electrical power problems. The scenario which involves Ahmad'computer, is related to the types of computer security risk which are Internet and network attack and system failure.

Internet and network attack is any information transmitted over networks has a higher degree of security risk than information on an organization's premises. There are five types of internet and network attack which is Botnets. Its can defined as a group of copromised compuer connected to a network. Second, Denial of Service Attack(DoS Attack). Its can be described as assault whose purpose is to disrupt computer access to an Internet services.

Third is a Back door which is a program or set of instruction in a program that allow users to bypass security controls when accessing a program, computer or network. Forth is Spoofing. Spoofing is a technique intruders use to make their network or internet transmission appear legitimate to a victim computer or network. Last but not least is Malware also known as malicious software. Malware is a programs that acts without a user's knowledges and deliberately alter the computer's operations. From the scenario, Ahmads'computer is attacked by malware.

Malware is divided to four types such as Computer Viruses, Worms, Trojan Horses and Spyware and Adware. Computer virus is a potentially damaging computer program that affects or infects a computer negatively by altering the way the computer works without the users' knowledges or permission.

Worms is a program that copies itself repeatedly foe example in a memory or an a network, using up resources and possibily shutting down the computer or network. Thirds is a Trojan Horses.

Its can be described as a program that hides within or looks like legitimate program. From the scenario, there is an ads that look legitimate but its not. Its is a virus that can caused the computer shut down by itself. The last one is Spyware and Adware. Spyware is a program placed on a computer wihout he users' knowledge that secretly collects information about the users. Adware also known as malvertising. It can be described as a program that displays an online advertisement in a banner or pop-up window on a web pages, on an online game or other internet services.

Malvertising is a hack cybercriminals use to spread malware via online advertisements. As we can see, malvertisements are deceiving and the damage can go beyond our website by infecting our computer with malware. From the scenario, an unwanted advertisement starts appearing on Ahmads' computer screen, so it has been victimized by adware. Cybercriminals use malicious advertisements to hack websites and computers. Sometimes they will inject malicious code into a legitimate advertisement. In these cases, malicious code is hidden in iframes, which are HTML elements that allow ads to appear on webpages.

Other times, they will create a malicious ad and use advertising networks to deliver the malware. When using a network, cybercriminals are able to insert their malvertisements across millions of websites at a time. Typically, users are infected by malvertisements in one of two ways. First, is by clicking on a

malicious ad. The click may prompt a pop-up warning the user that the users' computer has been infected. In order to " fix the issue," the user is asked to download software.

This is a tactic cybercriminals use to manipulate users into downloading malicious software onto their computer. The second method a hacker might use to spread malware is through the use of a drive-by download. This method does not require a user to click on an advertisement. Instead, the visitor is infected with malware simply by visiting a website hosting a malicious advertisement. All websites are malvertising targets, including high-profile sites.

For example, PerezHilton. com, a high-traffic popculturesite, fell victim to a malvertising attack in May 2016, its according from the website Lauren Papagalo, retrieved from https://www. sitelock. com/blog/2016/08/what-is-malvertising/. In this malvertising campaign, the cybercriminal inserted malicious code to an iframe. When visitors clicked on the malicious advertisement, they were redirected to an exploit kit that spread malware to the users' computers.

There are the ways to overcome the Internet and network attack which is by installing antivirus programs also called vaccines in our computer. The cost of antivirus software is much less than the cost of rebuilding the damaged files. An antivirus program is desingned to detect, disinfect and protect our computer and network from viruses and worms. Antivirus programs also work by looking for programs that attempt to modify the boot programs, the operating system or other programs that normally are read from but not

modified. In addition, many antivirus programs automatically scan files that we downloaded from the Web, e-mail attachments, opened files and all types of removable media inserted in our computer.

The popular antivirus program that usually used is AVG Anti-Virus, avast! Antivirus and McAfee VirusScan. Another tips for preventing viruses and other malware is back up your files often. Even with the best antivirus software, realize that our computer files can be infected. Second, be careful about what we downloading data as viruses and adware could be attached to our files and also disable autorun as viruses could install themselves automatically.

To reduce the risk of malvertisements is you should start by ensuring that your plugins and software are updated in order to reduce your risk. Older versions of plugins and content management systems (CMS) are access points for hackers and can be full of exploits. When you are running everything on the most updated version, you help prevent malware. Fourth, scan all software before using even if it is shrink-wrapped. Viruses have been found in manufacturer supplied software. Scan all removable media also a tip to preventing computer from involves with the viruses. USB flash drives and other removable storage devices are common culprits for carrying viruses from one computer to another computer and spreading viruses throughout networks.

For example, if someone hands you a removable storage device that has been used in another system, you must scan it first to avoid your computer from getting the viruses and other malware. Last but not least, avoid pirated,

illegal copies of copyrighted software. Not only using them illegal but they are a favourite source of viruses. For example, the online games that Ahmad played maybe come from the illegal downloading of the copyrighted software. So, his computer might had effected by the viruses so his computer will suddenly shut down by itself and when he try to switch on the computer, it takes longer time than normal.

Another computer security risk that happen in this scenario is system failure. System failure can occur because of a hardware failure or a severe software issues. It can causing the system to freeze, reboot or stop functioning altogether. A system failure may or may not result in an error being displayed on the screen. The computer may shut off without warning and without any error message. If an error message is displayed, it often is displayed as a Blue Screen of Death error.

System failures may result from a failing motherboard because the computer is not able to process requests or operate in general. Motherboard is the one of the most important components of a computer. It is because it holds all the components inside the computer that connects everything. The CPU is the brain of the computer while the nerve center connecting all the pieces and components together is the motherboard.

Any problem with the motherboard will definitely create problems with all the other components of the computer thus affecting its performance. Overheating of the computer also might be the effect of system failure. It is because Ahmad plays an online games hours and hours until he did not realised that the computer was overheating. Besides, heat related issues

occur when the computer is working hard such as playing a graphically intense computer likes Ahmad case. Overheating CPU caused by a temperature problem is definitely a bad sign. It can destroy the processor and can cause instsbilities in the hardware of the system.

A bad processor can causes a system failure because the computer cannot operate if the processor is not working properly or at all.. System failures also may result from a hard drive with bad sectors, causing the operating system to not be able to read data from the hard drive. A bad RAM chip can also cause system failures because the operating system is not able to access data stored on the RAM chip. System failures due to software issues can occur if the issue in the software, such as a bad line of code, is severe enough. The system failure and subsequent computer shut down occurs as an attempt to prevent damage to other software or the operating system.

Safeguards against system failure is create a backup or duplicate a files, programs or disk that can used if the original is lost. In case of a system failure or discovery of corrupted files, you restore the files by copying the backed up files to their original location on the computer. Keep the back up copies in a fireproof and heatproof safe or vault or offsite. Using the Uninterrupible Power Supply(UPS). UPS keeps the power running through a computer if there are electrical failures, by firstly storing a reserve of power then supplying the device with power for a short amount of time.

There are two types of UPS which is Standby UPS also called Offline UPS and Online UPS. Offline ups switch to battery power when power offline. Amount of time to continue using the computer depend on electrical requirement of

the computer and size of batteries. Offline UPS is less expansive compared to Online UPS. Online UPS always runs off the battery, which provides continuous protection. Besides, if the computer overheating, we must check whether all fans are running or not. It is possible that the fan is unplugged, reducing air flow. In addition, it is more important to monitor the amount of heat being generated inside the computer.

We can check our computer internal temperature to see if it is running too hot and in danger of overheating by using a free monitoring programs such as 'Wise System Monitor'. There are also some of the companies use duplicate components or computers to peotect against system failure. A fault-tolerant computer has duplicate components so that it can continue to operate when one of main components fail. For example, Airline reservation system, communications networks and automated teller machines is the system that duplicate components or computer to ensure that no data is lost the event of a system failure.

In conclusion, computers, networks, and databases play an ever-increasing role in fighting crime. Many computer criminals use computers and the Internet to stealing intellectual property. Some steal entire identities. Others use Trojan horses, viruses, worms, logic bombs, and other types of malware to sabotage systems. Normally, security measures serve to protect our privacy and other individual rights. But occasionally, security procedures threaten those rights.

The trade-offs between computer security and freedom raise important legal and ethical questions. Computer systems are not threatened only by

criminals they are also threatened by software bugs and hardware glitches. An important part of security is protecting systems and the people affected by those systems from the consequences of those bugs and glitches. Because our society uses computers for many applications that put lives and livelihoods at stake, reliability issues are especially important. In modern military applications, security and reliability are critical.

As the speed, power, and complexity of weapons systems increase, many fear that humans are being squeezed out of the decision-making loop. The debate over high-tech weaponry is bringing many important security issues to the public's attention for the first time. Some of the most powerful weapons in future wars will be software and hardware tools for disabling or destroying the information infrastructure we have come to depend on. So, computer security is important, primarily to keep our information protected. It's also important for your computer's overallhealth, helping to prevent viruses and malware and allowing programs to run more smoothly.

Reference

- Book

1. Gary B. Shelly and Misty E. Vermaat. (2012). Discovering Computers: Your Interactive Guide to the Digital World, Complete. CourseTechnology: Cengage Learning.
2. Gary B. Shelly, Thomas J. Cashman, Glenda A. Gunter and Randolph E. Gunter. (2006). Teachers Discovering Computers Integrating Technology and Digital Media in the Classroom. Thomson: Course Technology.

- Website

1. " PC Troubleshoting Tips." ComputerTipscom. N. p, n. d. Web. 10 Feb. 2016. Retrieved from http://www. computertips. com/pc-troubleshooting/
2. Sarapenina. What are various Internet and Network Attack, and how can users safeguard against these attacks?
3. September. 2014. Retrieved from https://cybersafety2014. wordpress. com/2014/09/11/what-are-various-internet-and-network-attacks-and-how-can-users-safeguard-against-these-attacks/
4. Computer Hope. System Failure. 17 October. 2017. Retrieved from https://www. computerhope. com/jargo/s/systemfa. htm