Internet and criminal activity

Technology, Information Technology

Explain how the Internet has aided criminal activity First Computer sciences and Information technology d Explain how the Internet has aided criminal activity. 1. Explain how the Internet has aided criminal activity Computer crimes involve any illegal act facilitated by the computer, whether this computer is used an instrument or object for the crime. E-commerce frauds, software piracy, and breaches of network security are the prominent types of the crimes on the internet. The detection of these crimes is hard as these crimes are afforded by the internet. Crimes make the user prone to the nuisance caused by any type of the crime because access of computer and the internet are now easier than before. Violating and offending the laws are also the crimes, but elevated technology increased the crime rates. Hacking is also most known crime in the current era of technology. This crime can be done anywhere in anytime. A computer is used to hack the bank, firm and houses by using the hacking skills. A new user of the internet is the target of the phishing. Hackers create the webpage that is identical to the shopping website. In the next, the hacker sends the link of the webpage to random users via emails. If a hacker is skilled the email is created similarly to the original format of the email. User clicks the given link and fills the personal information, such as credit card number, and other requirements. As the webpage is similar copy of the original website, it is rare pointed out that webpage is fake. Hacker server stores all information, and misuses the user’s information for making frauds (The Essay Blog 2009). 2. Provide three (3) specific examples of how the Internet has aided criminal activity Cyber crime: This is the activity, using the internet and computers to steal information or financial credits from business companies, banks or persons.

Billions of dollars are theft through cyber crime on the internet. Cyber-espionage is the example of the cyber crime, which is used to steal the personal information with commercial value. Industrial espionage: It accounts the stealing of competitors or individuals in achieving the information. In history, the unscrupulous companies spied on individuals and competitors. Cyber-Terrorism: it can be defined as the attacks on the part of the internet, in order to prevent users from using the legitimate internet based services. It is intended to engender fear in the supremacy of the attacking group or group behind the attack (Barrett, Steingruebl and Smith 2011). 3. Identify the types of crime that traditionally have been non digital in nature are now best abetted by Internet activity Current era of cybercrime is not accessing the computers via the internet for notoriety or fun. There has been a change in the criminal landscape. In the non digital era, the crime groups sought the haven from weak governments. Now the criminal groups are moving from the traditional, non digital crimes to more rewarding in the cyberspace. I. Online gambling is now more aided by the commuters via the internet than earlier times. Illegal gambling is not allowed anywhere in the world. Now a gambler sitting in home involves in the prohibited acts. This type of crime is beneficial for the crime organizers. II. Cyber stalking involves the use of technology to abuse the individuals online. In the non digital crimes era, the stalkers used the letters, physical contact or calls to harass the other person. Now, the stalker is more comfortable through computers via the internet. III. Terrorism is another form of crime, which is now easier for giving instructions to members via the internet. IV. Theft of propriety or Information. In non digital crime, the information theft of a person or

corporation was done by using the physical involvement. Now the computer aided technology via internet steals the confidential information of individuals as well as corporations (Schmalleger, 2009). 4. Describe the role viruses, other malicious code, and phishing attacks play in aiding this criminal activity Role Viruses: Threat messages are combined to attack individuals, business, organization and e-Commerce. They include the email born spyware, adware, denial of service (DoS) attacks and directory harvesting attacks. The viruses programs cause the abnormal functioning of the legitimate users to their computer systems. In 1999, the “ Melissa” virus infected more than 1. 2 million computers in Europe, and US Business and resulted into a damage of 80 million dollars (Kunz and Wilson 2004). Malicious Code: Type of phishing as content-injection phishing details the situation, when a hacker makes changes in contents of a legitimate (official, company) website and misleads the users in giving their very confidential information. For example, hacker inserts the malicious code to retrieve the log in information and credentials of the users. Trojan used as malicious code controls the actions of stealing the identity of users (Bandy and Qadri, 2007). Phishing Attacks: Phishing attacks are used to tell about the technical ploys and spoof emails. It is intended to trick the recipient to give personal or company’s information about account details and security information. The hacker sells out the property to a third party via the special chat rooms. Hacker sells the information and reduces the risk of apprehension. A large number of deceptive emails are sent by the scammers and fraudsters to the random users of the internet. The phishing emails look like a realistic and professional and user shows accepting behavior to enter the information on

given web page links sent via these emails. References Banday, M. T., Qadri, J. A. (2007), “ Phishing - A Growing Threat to E-Commerce,” The Business Review, ISSN: 0972-8384, 12(2), pp. 76-83. Barrett, M., Steingruebl, A., and Smith, B. (2011). Combating Cybercrime, Principles, Policies and Programs, Available from https://www. paypalmedia. com/assets/pdf/fact_sheet/PayPal_CombatingCybercrime_WP_0411_v4. pdf Accessed on 18/11/2012. Kunz, M., and Wilson, P. (2004). Computer Crime and Computer Fraud, University of Maryland Department of Criminology and Criminal Justice Fall, 2004. Schmalleger, F. (2009). Criminology today: An integrative introduction. New Jersey: Pearson Education inc. The essay Blog (2009). Technology Does More to Increase Crime That to Solve It. Available from http://theessayblog. wordpress. com/2009/05/20/technology-does-more-to-increase-crime/ Accessed on 17/11/2012.