How the internet has aided criminal activity

Running Head: CRIMINAL ACTIVITIES Criminal Activities through the Internet School How did the internet help in the execution of criminal activities? Modern information technology, such as the internet has initiated new forms of crimes and made perpetration of old felonies effortless. Computer crimes may involve identity theft, cyberstalking, scams and frauds, hacking, creation of malicious codes, child pornography, and violation of copyrights. Criminals use computers to facilitate the embezzlement of money and properties; theft of confidential records; and alteration and destruction of valuable files. The misuse of the computer may involve the falsification of computer signatures through unauthorized codes; the creation of false bank accounts; theft of personal information and misuse of the stolen information; the virus infection created on computers that can hamper the proper software operations and damage records (Computer-Based Crime, 2011). This paper will give specific examples of criminal activities through the use of computers and the internet; will cite how yesterday’s non-digital crime, as in the case of pornography, has become today’s menacing digital crime; and will discuss some types of computer crimes, such as identity theft, phishing scam, virus and malicious software.

Specific Examples of Criminal Activities through the Internet

September 11 Attack. The execution of the September 11 attack on the World Trade Center, which claimed an estimated 3, 120 lives from over 90 countries around the world, (US Department of State, 2002), is a form of cyberterrorism. Cyberterrorism is the unauthorized attack and risk against computers, networks, and the stored information purposely executed to threaten or force a government, a nation or its people to advance one’s political or social intentions. Cyberterrorist attacks demonstrate power and

aggressively threaten or harm persons or property (Denning, 2000).

Juvenile Computer Hacker Disabled FAA Tower at Regional Airport. In Boston, Massachusetts, a juvenile hacked the computer system of a telephone company servicing the Worcester Airport. A series of commands sent from the hacker’s computer immobilized the FAA control tower for six hours in March 1997 (US Department of Justice, 1998).

Release of Computer Worm Attacked Microsoft Corporation. In September 2003, a juvenile was arrested for releasing a variant of the Blaster computer worm that directly infected computers worldwide to commence a distributed denial of service attack against the Microsoft Corporation (US Department of Justice, 2003).

Pornography and Pedophilia: Yesterday’s Non-Digital Crimes are now Digital Crimes

More than four decades ago, open, unusual or violent pornography was restricted to adult bookstores and movie houses. It could be only be viewed and circulated in adult comic books, magazines, " peep shows," and bold films. Pornography characters were mandatorily exposed in public, jeopardizing their identity and humiliation. The unparalleled heave of technological innovation gave us videos, pay-per-view cable television, satellite connections, compact disks, and the Internet. Such mediums provided fresh, personal and a more peculiar approach to use obscenity. Today, through the internet, pedophiles and other sex offenders, concealed behind screen names or aliases, communicate very openly and unreservedly with one another. They meet online and exchange child pornographic images and videos, share or swap strategies to contact and entice minors online (Hughes, 2001).

Computer Crimes

Identity Theft

Identity theft is the pilfering and illegal use of private information from an unsuspecting individual to access personal financial accounts. The targeted personal data include a victim’s address, birth date, telephone number, social security number (SSN), bank account number, credit card number, or other valuable identification records to be used for the thief’s economic gain. Criminals use this information in opening new credit and depository accounts, applying for home or car loans, leasing homes, apartments or vehicles (Brody, Mulig & Kimball, 2007) applying for benefits, or filing fake tax returns (Palmer, 2006).

Phishing Scam

Phishing is a scam that uses volumes of electronic mail messages to attract innocent victims into disclosing private information. A phishing email illustrating a believable problem lures the victim to a fake link that is a replication of the victim’s bank web address; the victim then fixes the imaginary concern and verifies account information and divulges personal identification. Subsequently, the phisher uses the pilfered PIN number, secret code, and identity to drain the victim’s bank account (Brody, Mulig & Kimball, 2007).

Viruses and Malicious Software

A virus is unknowingly downloaded on a victim’s computer. This process is known as pharming which is a technically higher form of phishing. The prey keys in a genuine web address but is instead redirected to a mock site. The pharmer then steals the financial account number, password, or other valuable information supplied at the phony web site (ID thieves preying on

consumers with new phishing scam called pharming, 2005).

A malware or malicious software is involuntarily installed to gain access to a computer system without the victim opening an attachment or clicking on a link. Simply opening a pharmers electronic mail or email message will directly download the secret program, forwarding the internet browser to a mock location (Hicks, 2005).

References

Brody, R. G., Mulig, E., & Kimball, V. (2007, September 1). Phishing, Pharming and Identity

Theft. Academy of Accounting and Financial Studies Journal.

Computer-Based Crime (2011). Idea Connection. Retrieved February 18, 2012 from

http://www. ideaconnection. com/solutions/505-Computer-based-crime. html

Denning, D. (2000, May 23). Cyberterrorism. Testimony before the Special Oversight Panel of

Terrorism Committee on Armed Services, US House of Representatives. Retrieved February 19, 2012 from

http://www. cs. georgetown. edu/~denning/infosec/cyberter ror. html

Hicks, D. (2005). Phishing and Pharming: Helping consumers avoid Internet fraud.

Communities and Banking. Retrieved February 19, 2012 from ABI Inform database.

Hughes, D. (2001). Sexual Predators Online. Protect Kids. Retrieved February 19, 2012 from

http://www. protectkids. com/dangers/onlinepred. htm

ID thieves preying on consumers with new phishing scam called pharming

(2005, October).

PRNewswire. Retrieved February 18, 2012 from

http://www. nclnet. org/news/2005/phishing_10132005. htm

Palmer, S. (2006, January 10). IRS warns consumers of e-mail scam. St. Petersburg Times.

Retrieved February 18, 2012 from ProQuest database.

U. S. Department of Justice (1998). Juvenile Computer Hacker Cuts off FAA Tower at Regional

Airport. Federal Computer Crime Cases Involving Teens. Computer Crime & Intellectual

Property Section. United States Department of Justice. Retrieved February 19, 2012 from

http://www. cybercrim e. gov/cases. htm

U. S. Department of Justice (2003). Juvenile Arrested for Releasing Variant of Blaster

Computer Worm That Attacked Microsoft. Federal Computer Crime Cases Involving Teens. Computer Crime & Intellectual Property Section. United States

Department of Justice. Retrieved February 19, 2012 from

http://www. cybercrim e. gov/cases. htm

U. S. Department of State (2002). September 11, 2001: Basic Facts.

Retrieved February 19, 2012from http://www. state.

gov/coalition/cr/fs/12701. htm