Code of Ethics

Jacob Silva, Network Security

University of Advancing Technology

CASE IN POINT

In the case of U.S. v. Livingston, et al., U.S. District Court, District of New Jersey, a Florida man was found guilty of a spamming scheme that used stolen email accounts. Timothy Livingston, age 31, of Boca Raton, Florida, was found guilty of an identity-theft scheme that hijacked customer email accounts to send unsolicited or spam emails that generated more than $1.3 million in illegal profits. He used his business "A Whole Lot of Nothing LLC" in early 2011 that specialized in sending emails or spam on behalf of its clients. His clients included such legitimate businesses such as Comcast Corporation, and insurance companies that sent out bulk emails to advertise their business, as well as online pharmacies that sold narcotics without prescriptions.

He was able to mask his online presence with proxies and bots in his botnet to remain anonymous. As part of this deception, he sent out massive amounts of spam without identifying himself as the sender. Livingston started using proxy servers and created a program to send out spam messages to further conceal his identity. He breached an email server and stole the confidential business information of victims, including databases of millions of Americans he could further his spam campaign.

In connection with his plea agreement, Livingston pled guilty to one count each of conspiracy to commit fraud in connection with computers and access devices, conspiracy to commit fraud in connection with electronic mail, and aggravated identity theft. He was sentenced and served 48 months in prison.

It is my belief, as a result of his abuse of his position with his clients and misusing the trust given to him, that jail time is highly warranted for exploiting for profit. It is not ethical to scam businesses, people, or companies for profit or gain.

CODE OF ETHICS

I.

DO NOT USE COMPUTERS TO HARM OTHERS.

It is unethical to use a computer to harm any user by means of hacking, spoofing, spamming, phishing, exploiting, or cyber bullying. This may include intentionally corrupting other user's data or files. It is not only wrong, but also illegal, to use a computer to steal someone else's personal information. It is unethical to create programs which are designed to steal, copy, or gain unauthorized access to other users' data. Also, manipulating or destroying files of another is unethical and should never be done unless upon request of the owner.

An example of something that violates Rule 1 would be abusing your use of the computer to conduct illegal activity for personal profit or gain. This may include inciting violence or participating in schemes to perpetuate illegal activity.

<u>CODE OF ETHICS</u>

II.

DO NOT ACCESS FILES

WITHOUT THE PERMISSION OF THE OWNER.

It is unethical to access someone's files without their permission. This includes spying on another person's data. This action is similar to breaking into someone's home and snooping through their personal belongings. Unsolicited access to someone's computer is very invasive to the person's privacy. This is an unethical violation of a person's privacy. An exception might be when spying is done out of necessity by an intelligence agency working a cybercrime case. In this instance, it cannot be considered unethical if backed up by law.

We know it is wrong to open someone's personal letters, so why would it be appropriate to read someone else's computer files or emails?

CODE OF ETHICS

III.

DO NOT USE COMPUTERS TO STEAL OTHER'S INFORMATION.

It is unethical to steal information using computer technology. Stealing others information through computers can be the equivalent to robbery. This would include obtaining private information about someone's bank account to conduct illegal activities such as unauthorized wire transfers from their accounts. It would also be wrong to acquire unauthorized data from an employee or a medical patient's history from. Accessing such personal and private information is illegal and, therefore, unethical.

Technology now makes it easier than ever to steal people's private information and to store or sell it for profit.

<u>CODE OF ETHICS</u>

IV.

DO NOT ILLEGALLY COPYRIGHT SOFTWARE

It is unethical to use copies of software or pirated copies without the consent from the owner. This would include movies, games, music, and software. This is illegal activity and infringes upon copyright laws meant to protect the programmer's or artist's work. Unless the creators give explicit permission to use their copyrighted material, it is unethical and illegal to obtain their copyright work.

An example of breaking this code of ethics would be to illegally download content such as music or movies that are intended to be purchased.

<u>CODE OF ETHICS</u>

V.

USE THE INTERNET ETHICALLY

It is unethical to be disrespectful and discourteous to your fellow users. This would include profanity, vulgarity, and downright disrespect. Interaction on the internet should be restricted to treating others with courtesy while communicating. It is also morally wrong to make false statements or accusations about others, causing emotional or psychological harm.

We should be open to helping one another, if they don't know how to do something. Since we have all started somewhere in the computer world, we should be open to helping one another to increase our own understanding. It is beneficial because it helps to reinforce what we already know.

Social etiquette in the real world applies in the computer world.

References

Florida Man Sentenced for Hacking, Spamming Scheme that Used Stolen Email Accounts. (2017,

February 16). Retrieved January 28, 2018, from https://www.justice.gov/opa/pr/florida-man-

sentenced-hacking-spamming-scheme-used-stolen-email-accounts

(n.d.). Retrieved January 28, 2018, from https://www.justice.gov/usao-nj/file/799351/download

Three Men Arrested In Hacking And Spamming Scheme; Targeted Personal Information Of 60

Million People. (2015, December 15). Retrieved January 28, 2018, from

https://www.justice.gov/usao-nj/pr/three-men-arrested-hacking-and-spamming-scheme-

targeted-personal-information-60-million