Computer Forensics Preparation

Cyberstalking is online harassment in which someone continually threatens, harasses, or intimidates another person using the internet or other digital communications technology. It can take many forms, such as sending threatening or abusive messages, spreading false rumors or lies about the victim, monitoring the victim's online activities, and even hacking into the victim's computer or social media accounts.

Cyberstalking is a serious and growing problem in the digital age. The internet and other digital communication technologies have made it easier for people to connect, but they have also made it easier for individuals to engage in harmful behaviors. Cyberstalkers can use a variety of tactics to intimidate and harass their victims, which can have a profound and lasting impact on the victim's mental health and well-being.

Some cyberstalkers use social media platforms to harass their victims, creating fake profiles to impersonate the victim or posting false information about them. Others may use email or instant messaging to send threatening or abusive messages. Some may even go as far as hacking into the victim's computer or social media accounts, stealing personal information, or using it to further their harassment.

The effects of cyberstalking can be devastating. Victims may feel a sense of constant fear and anxiety, as they are never sure when the cyberstalker will strike next. While cyberstalkers might watch their online activities and even track their actual movements, they might lose their sense of privacy. Cyberstalking can, in severe circumstances, result in physical damage or even death.

Recognizing the signs of cyberstalking and taking steps to protect oneself is essential. This can include blocking or reporting the cyberstalker, changing passwords frequently, and limiting the amount of personal information shared online. It is also essential to seek support from friends, family, or a professional counselor if one is a victim of cyberstalking, as it can be a traumatizing experience. I gave the student an explanation of the Oath of the Four Amendments of the United States of America.

I started my research on Cyberstalking law in the State of New Jersey. The crime of Cyberstalking is defined in section 2C:33-4.1 of the New Jersey Code of Justice. Section 2C:33-4.1 also requires evidence of "intent" to cause fear or emotional harm, and, depending upon the circumstances, proving subjective intent can be a substantial burden for the prosecution. For cyberstalking, you are dealing with a fourth-degree indictable offense with the potential for up to 18 months of imprisonment and a $10,000 fine.

Regarding Cyberstalking in New Jersey, it is a criminal offense defined in section 2C:33-4.1 of the New Jersey Code of Justice. To prove Cyberstalking, the prosecution must show that the defendant engaged in the course of conduct intended to cause fear or emotional distress to the victim and that this conduct did cause fear or emotional distress. This can include sending threatening or harassing messages, creating fake social media accounts to impersonate the victim, or monitoring the victim's online activity.

It is a criminal offense defined in section 2C:33-4.1 of the New Jersey Code of Justice. To prove Cyberstalking, the prosecution must show that the defendant engaged in the course of conduct intended to cause fear or emotional distress to the victim and that this conduct did cause fear or emotional distress. This can include sending threatening or harassing messages, creating fake social media accounts to impersonate the victim, or monitoring the victim's online activity.

Students need to understand the laws regarding cyberstalking and the potential consequences of engaging in this behavior. By educating themselves on the issue, they can better protect themselves and others from this form of online harassment.

While investigating, I got on Twitter and used the Metadata Field to gather information. Instant messages between the cyber stoker and the student. I have captured the user screen names, timestamps, and the messages between the cyber stoker and the student and tracked the stoker's Geo-location where the user sends from what device and the location where the stalker sent it from for the right authorities to arrest the individual(s).

This is how metadata is the information that describes other data. In digital communications, metadata can include timestamps, IP addresses, and geolocation data. This information can be invaluable in the investigation of cyberstalking, as it can provide essential clues as to the identity and location of the cyberstalker.

By analyzing the time stamps of the messages and the geolocation data, you could track the cyberstalker's movements and determine where they were when they sent the messages. This information can be critical in building a case against the cyberstalker and providing evidence to law enforcement for an arrest.

It is important to note that gathering and analyzing metadata can be a complex process that requires specialized knowledge and tools. It is also essential to ensure that any metadata gathered is obtained legally and ethically and that the privacy rights of all parties involved are respected. Metadata can be a valuable tool in investigating cyberstalking and other forms of online harassment. By leveraging this information, investigators can more effectively track down and hold accountable those who engage in these harmful behaviors.

In conclusion, cyberstalking is a severe form of online harassment that can devastate victims. The laws regarding cyberstalking vary by state but generally require evidence of intent to cause fear or emotional harm. Gathering and analyzing metadata can be an essential tool in the investigation of cyberstalking, as it can provide valuable information about the identity and location of the cyberstalker. However, ensuring that any metadata gathered is obtained legally and ethically is essential. By educating ourselves on the issue of cyberstalking and leveraging tools like metadata, we can better protect ourselves and others from this deadly form of online behavior.

Resources

Hinduja, S. (no date) *Cyberstalking*, *Cyberbullying Research Center*. Available at: https://cyberbullying.org/cyberstalking (Accessed: April 7, 2023).

New Jersey Cyberstalking Lawyer: Defense attorneys: Gorman Law FIRRM (2021) *The Gorman Law Firm*. Available at: https://www.gormanlawfirmnj.com/areas-of-practice/domestic-violence/cyberstalking/ (Accessed: April 7, 2023).

Forensic Focus, Hall, A. and Nazim, M.A.B.M. (2020) *Key twitter and Facebook metadata fields forensic investigators need to be aware of*, *Forensic Focus*. Available at: https://www.forensicfocus.com/articles/key-twitter-and-facebook-metadata-fields-forensic-investigators-need-to-be-aware-of/ (Accessed: April 7, 2023).