Name of Student

Name of Professor

Course

Date

Cyber Crimes

Cyber crimes are criminal activities perpetuated through the internet and constitute activities such as cyber bullying, phishing, and online child abuse. Federal authorities have invested heavily in resources to deal with the identified issues. This essay is going to discuss various prevalent criminal activities created with the advancement of cyber technology. Additionally, it will also evaluate how investigators respond to these issues.

*Cyber bullying*

Cyber bullying can be termed as the activity whereby an individual or a group of persons engage in menacing, harassing, or offensive deeds through the application of technology (Foody, Samara, and Carlbring 236). Furthermore, Foody, Samara and Carlbring continue to assert that prominent examples of cyber bullying encompass: sending unwarranted messages, intimidating individuals online, posting demeaning images, videos, or messages online (236-238). A unique characteristic of cyber bullying is the crime’s anonymity. This statement means that the perpetrators of the crime can promote their illegitimate activities while remaining unknown. This element is highly detrimental to the victims because it heightens the probability that the perpetrator will evade punishment (Foody, Samara, and Carlbring 235-238). Since the perpetrator is unidentified, the probability of facing justice is low until that time they will be known.

In the U.S., about 20.8 percent of students have experienced bullying according to the National Center for Educational Statistics (Pacer’s National Bullying Prevention Center).

In dealing with cyber bullying, different countries have different approaches. For example, UK has implemented anti-bullying policies aimed at preventing bullying in learning institutions. However, there is a slow implementation of these policies in the UK schools based on the 23 percent augmentation that ranges from the 8.5 percent to 32 percent between 2002 and 2008 (Foody, Samara, and Carlbring 238).

In the U.S., states have different policies of dealing with cyber bullying, and the government stipulates the measures that need to be taken to deal with cyber bullying. The U.S. government stipulates how victims of cyber bullying should report it to law enforcement. Based on the understanding that some cyber bullying forms are considered criminal in some states, the government highlights the need to consult available state regulations for proper guidance (Stopbullying.gov(*a*). Since students are at high risks of being subjected to cyber bullying due to their young age and innocence, the government stipulates the measures to be taken to deal with cyber bullying in schools. Schools need to use their policies to deal with bullying, while being guided by their state regulations (Stopbullying.gov(*a*). Concerning cyber bullying in schools, the U.S. Department of Education played significant roles of reviewing state laws to provide guidelines of how the learning institutions could deal with the issue based on their state (Stopbullying.gov(*b*).

*Phishing*

Phishing is the process where criminals deceive people to provide their financial or personal details (Jagatic, Johnson, Jakobson, and Menczer 94). Many people can be vulnerable to phishing because the messages pretend to originate from legitimate firms such as banking institutions (Aburrous, Hossain, Dahal, and Thabtah 7913-7921). However, once a victim clicks on those messages, important client information is accessed by the sender, and it can lead to worse damages such as identity theft. It is possible for phishing to attract police attention particularly when criminal activities such as identity theft or hacking and loss of money, especially through online banking platforms (Aburrous, Hossain, Dahal, and Thabtah 7913-7921). The government plays its role of ensuring its citizens are informed about the most appropriate ways of avoiding phishing while working online. However, it is worth noting that the process of identifying and apprehending the perpetrators of such activities is challenging because of the anonymity of the perpetrators (Foody, Samara, and Carlbring 235-238).

It is worth noting that some of the crimes linked to identity theft encompass banking fraud, document fraud, and credit card fraud among others (Reyns 217). Cases of identity theft are prevalent in many countries among them United Kingdom and the U.S. In the United Kingdom, for example, about £212.6 million was lost in card fraud in 2006, which was a 16 percent increase from 2005 (Reyns 217). Furthermore, it is worth noting that about 1.8 million citizens in Britain are affected by identity crimes and these crimes cost the country about £2.7 billion. Reyns continues to assert that this amount is quite extensive because it is equal to about £1000 in monetary gain from every identity that is stolen (217).

It can be observed that some of the greatest costs suffered through phishing are financial in nature. Banking institutions are forced to engage in technological measures to ensure they cushion their businesses and clients against e-banking phishing (Aburrous, Hossain, Dahal, and Thabatah 7915-7921). Based on the understanding that malicious people generate phishing messages with the intention of mimicking genuine banking websites, banking institutions have formulated strategies to ensure that clients do not lose money through the fraudsters. Fraudsters, according to Aburrous, Hossain, Dahal, and Thabtah (7913), appear to be highly experienced and those involved in investigating the crimes also have to be highly experienced. Banking institutions rely on information technology experts who have unique understanding of how phishing takes place. In banking institutions, for example, the need to conduct data mining has been critical in ensuring that they can detect phishing before it takes place (Aburrous, Hossain, Dahal, and Thabatah 7915). Through these data mining techniques, the banking experts can detect specific websites that are highly likely to undertake phishing activities based on their algorithms. Then, the acquired information is subjected to the fuzzy law engine to assist in providing the exact rate of phishing output (Aburrous, Hossain, Dahal, and Thabatah 7919-1921).

*Children and online sexual exploitation*

Globally, children are vulnerable to online sexual exploitation mainly due to the emergence of new technologies (U.S. Department of State). The advancement of mobile device technology and additional gadgets such as web cameras, children have become vulnerable to online exploitation, particularly for sexual purposes. Additionally, child abusers also take advantage of apps to target, coerce, and recruit children to participate in sexual activity in different global parts (U.S. Department of State).

A study in the U.S. revealed that out of twelve children, one had been sexually victimized (Mitchell, Jones, Finkelhor, and Wolak 44). Additionally, a survey carried out by the National Crime Victimization revealed that in 2004, teenagers’ victimization rate (those between the ages of 12 and 15 years) surpassed the national rate’s average by over two times (Mitchell, Jones, Finkelhor, and Wolak 44). It is worth noting that children can be subjected to sex crimes through the internet by strangers, acquaintances, and family members.

Since the issue involves children, it is highly sensitive and various organizations have invested heavily to ensuring that the perpetrators are arrested and punished. For example, the U.S. Department of Justice has funded several task forces, whose number grew to 61 from 30 between 2000 and 2009 (Mitchell, Finkelhor, Jones, and Wolak 416. Additionally, states also have relevant law enforcers who liaise with prosecutorial agencies to ensure the criminals are punished. To achieve this objective, a section of law enforcers serve as undercover agents where they spend considerable time online, whereby they impersonate minors with the intention of identifying the perpetrators and eventually arresting them (Mitchell, Finkelhor, Jones, and Wolak 417). By impersonating minors, the undercover agents can lure the perpetrators into eventually meeting them, where they are arrested and prosecuted.

Additionally, there is the Interpol which also plays imperative roles of ensuring that perpetrators are arrested and punished. The Interpol takes note of films and photographs that have been used online portraying sexual abuse among children to identify probable victims (Interpol). Furthermore, the Interpol works together with other law enforcers to identify probable victims and rescue them, while also ensuring the abusers receive the desired punishment (Interpol). It is worth noting that the Interpol carries its objectives globally to ensure the perpetrators are curtailed from expanding their network and punishing them.

Therefore, it can be observed that the development of the internet has its merits and challenges. Whereas the internet can be used to achieve positive gains, there are individuals who use it for negative reasons such as cyber bullying, phishing and email scams, identity theft and online child abuse. However, relevant law enforcers are keen to ensure the perpetrators are punished.

Works Cited

Aburrous, Maher, M. A. Hossain, Keshave Dahal, and Fadi Thabtah. “Intelligent phishing detection system for e-banking using fuzzy data mining.” *Expert Systems with Applications*, vol. 37, no. 12, 2010, pp. 7913-7921.

Foody, Mairéad, Muthanna Samara, and Per Carlbring. “A review of cyberbullying and suggestions for online psychological therapy.” *Internet Interventions,* vol. 2, no. 3, 2015, pp. 235-242.

Interpol. *Victim identification*. Author, 2018, [www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification](http://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification). Accessed 14 Sep. 2018.

Jagatic, Tom, Nathaniel Johnson, Markus, Jakobson, and Filippo Menczer. “Social phishing.” *Communications of the ACM*, vol. 50, no. 10, 2007, pp. 94-100.

Mitchell, Kimberly, David Finkelhor, Lisa Jones, and Janis Wolak. “Growth and change in undercover online child exploitation investigations, 2000-2006.” *Policing & Society,* vol. 20, no. 4, 2010, pp. 416-431.

Mitchell, Kimberly, Lisa Jones, David Finkelhor, and Janis Wolak. “Internet-facilitated commercial sexual exploitation of children: Findings from a nationally representative sample of law enforcement agencies in the United States.” *Sexual Abuse: A Journal of Research and Treatment,* vol. 23, no. 1, pp. 43-71.

Pacer’s National Bullying Prevention Center. *Bullying statistics*. Author, Dec. 27, 2017, [www.pacer.org/bullying/resources/stats.asp](http://www.pacer.org/bullying/resources/stats.asp). Accessed 14 Sep. 2018.

Reyns, Bradford. “Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses.” *Journal of Research in Crime and Delinquency*, vol. 50, no. 2, 2013, pp. 216-238.

Stopbullying.gov(*a*). *Cyber bullying.* Author, Feb. 8, 2018, [www.stopbullying.gov/cyberbullying/how-to-report/index.html](http://www.stopbullying.gov/cyberbullying/how-to-report/index.html). Accessed 14 Sep. 2018.

Stopbullying.gov(*b*). *Law and policies*. Author, September 8, 2017, [www.stopbullying.gov/laws/index.html](http://www.stopbullying.gov/laws/index.html). Accessed 14 Sep. 2018.

U.S. Department of State. *Online sexual exploitation of children: An alarming trend*. Author, 2017, [www.state.gov/j/tip/rls/fs/2017/272010.htm](http://www.state.gov/j/tip/rls/fs/2017/272010.htm). Accessed 14 Sep. 2018.