Cybercrime has become a common method to enact crimes, and it occurs when criminals use the internet to commit illegal activities. The purpose can be related to stealing users’ identity, exploit sexually, or to arrange cyber-attacks. According to Travis (2015), in the last year, there have been many online fraud events that reached to 5.1 million. More than five hundred pounds are lost from 37% of fraud victims, and five thousand pounds by one 1% in 2011 to 2014 (ibid). This essay will be functioned by recent studies and statistics that are related to cybercrime; constrained to identity theft, child pornography, and cyber-terrorism. It will examine the effects of cybercrime, and how to prevent cyber-criminals who are involved in identity theft, child pornography, and cyber-terrorism activities that could be harmful for internet users.

Firstly, online identity theft is an illegal activity that may harm internet users by stealing their personal information to assume their identity; however, this issue could be prevented by being cautious on providing personal information on the web. Hackers who are professionalised in this type of cybercrime are called phishers derived from the word fishing. However, it starts with letter P then H to show that this activity is based on imitation, to trick the victims and steal their personal information (Jakobsson and Myers 2007). According to the BBC (2015), from January to March of 2015, the amount of users who are affected by identity theft has increased by 31%, and the median age among those victims was 48 years old. Hence, more victims are going to be affected negatively, and most likely financially through their stolen identities to buy items online or to open bank accounts and credit cards by phishers. Therefore, the victims might receive unfamiliar bills of products that they have not purchased. There are two effective solutions that could counter this problem. Firstly, the danger of providing personal information on social media (BBC 2015). The user does not need to type in detailed information that could lead phishers to mimic their identity, and then commit illegal activities. Secondly, is to switch the viewable settings from public to private whenever it is possible (Neate 2013). Especially, if the website is popular such as Facebook or Instagram, this method prevents the phishers accessing users’ personal information. In addition, there are specialized organizations that deal with fraud and identity theft in the UK, and reporting to the right authorities such as UK’s national reporting centre could be helpful (Neate 2013). As a result, between 2011 and 2014 the percentage of the unauthorised access to personal information increased to 8% among other cybercrime activities, after one year the percentage decreased to 6% (ONS 2015). However, these solutions might not be adequate to avoid the problem completely.

Furthermore, online crimes can involve serious and sensitive problems such as child exploitation; however, police governments and parents’ responsibility over their child can prevent this issue. Paedophiles started using the internet to contribute sexual contents with others who have the same interests, and this has started to become a major problem since the middle of the nineties (Akdeniz 2008). Technology has made the accessibility to child pornography easier; for instance, blackmailing children to encourage them to post sexual contents. Being sexually abused as a child may have significant consequences. Depression is one of the symptoms that children might feel after sharing sexual images with the other peer, which it could also leads to committing suicide (Munro 2011). According to The Lantern Project (2012), almost 55 thousands sexual crimes happened in England and Wales between the periods 2010 to 2011 towards children who are aged under than 16 years old (ibid). The issue of child pornography can be prevented by the government and the parents of the child. The government could block websites that have sexual child contents, and track the source of these websites. Therefore, this solution could lead to arrest the individuals who are involved in this type of cybercrime. Moreover, the materials of child pornography have been removed by the police and the Child Exploitation and Online Protection Centre from 18% in 1996 to less than one percent in 2013 (House of Commons 2014). The second solution involves parents’ responsibility, and it starts with having a conversation about surfing the internet safely (Dredge 2014). An effective way to obtain the children attention is by discussing the safe side of the internet and the unsafe side of it, to make them aware of the websites that they visit (ibid). In addition, a company such as Vodafone has supported this idea by providing recommendations to parents about surfing the web safely (House of Commons 2014).

A very severe problem which could affect businesses and governments negatively is cyber terrorism; however, upgrading security systems and educate the employees more about polices and protection might reduce the damage of the next cyber-attacks. Every year, the United Kingdom economy faces cyber-attacks that cost them over 27 billion pounds (Oxford Economics 2014). Companies may be harmed financially by increasing the cost of their business in order to develop the security, and they also might gain bad repetitions if they dealt with cyber-attacks (CESG 2015). A study shows that there has been many reports came from 81% of great companies about having security breaks, costing them 600,000 pounds to 1.5 million pounds on median (ibid). Improving cyber security might reduce the damage of the cyber-attacks; for instance, upgrading the operating system of the company and installing anti-viruses programs are methods to prevent any suspicious sources attach with the company’s business (Beggs 2004). Furthermore, educating the employees about the regulations of the company, and individual protections might be a huge role to prevent cyber-attacks. To protect the employees and manager’s information; education can be an effective solution. Employees and managers might need to obtain loads of knowledge about the security operation in order to protect the company’s information (Beggs 2004). Moreover, the UK government stepped ahead after the Paris attack that happened on the 13th of November 2015 (Wright 2015). George Osborne claims that the terrorist organization (ISIS) is planning to commit cyber-attacks on the UK; therefore, many jobs are related to undertake these electronic attacks towards the United Kingdom were offered by the National Cyber Centre (ibid).

In Conclusion, it has been demonstrated that the internet could be used to: stealing personal information of the users on the internet, share sexual child contents, and it also could be a place for cyber-terrorists to arrange attacks on countries and companies. Therefore, studies recommend focusing on developing the internet security and monitor children while they are browsing the internet. In addition, governments have big impacts on improving and protecting the citizens from cyber criminals. This essay has been limited on cybercrimes, and the problems of it were analysed by some statistics and studies that occurred in the United Kingdom. Therefore, the results of this essay shows that the government could raise awareness around this topic by education, and how it could harm families’ lives and damage business and organizations.

Reference List :-

Akdeniz, Y. 2008. *Internet child pornography and the law*. Burlington, VT: Ashgate.

BBC News. 2015. *Number of identity theft victims 'rises by a third'* [Online]. Available at: http://www.bbc.co.uk/news/uk-32890979 [Accessed: 28 November 2015].

Beggs, C. and Butler, M. 2004. *Developing New Strategies to Combat Cyber-Terrorism* [Online]. Available at: http://www.irma-international.org/viewtitle/32381/ [Accessed: 2 December 2015].

CESG. 2015. *Common Cyber Attacks: Reducing The Impact* [Online]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment\_data/file/400106/Common\_Cyber\_Attacks-Reducing\_The\_Impact.pdf [Accessed: 1 December 2015].

Dredge, S. 2014. *How do I keep my children safe online? What the security experts tell their kids* [Online]. Available at: http://www.theguardian.com/technology/2014/aug/11/how-to-keep-kids-safe-online-children-advice [Accessed: 1 December 2015].

House of Commons. 2014. *Online safety*. London: authority of the House of Commons.

Jakobsson, M. and Myers, S. 2007. *Phishing and countermeasures*. Hoboken, N.J.: Wiley-Interscience.

Munro, E. 2011. *The protection of children online: a brief scoping review to identify vulnerable groups* [Online]. Available at: http://www.saferinternet.org.uk/content/childnet/safterinternetcentre/downloads/Research\_Highlights/Munro\_OnlinevulnerabilityReporttoDFE-Final-October2011.pdf [Accessed: 22 November 2015].

Neate, T. 2013. *How to prevent identity theft* [Online]. Available at: http://www.bbc.co.uk/consumer/22342924 [Accessed: 24 December 2015].

ONS, 2015. *Proportion of adult internet users experiencing negative online incidents, Year ending March 2011 to Year ending March 2015 CSEW* [Table]. Available at: http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/rft-table-5---supplementary-tables.xls [Accessed: 21 November 2015].

Oxford Economics. 2015. *Cyber-attacks: Effects on UK Companies* [Online]. Available at: https://www.cpni.gov.uk/documents/publications/2014/oxford-economics-cyber-effects-uk-companies.pdf?epslanguage=en-gb [Accessed: 3 December 2015].

The Lantern Project. 2012. *Statistics on child sexual abuse* [Online]. Available at: http://www.lanternproject.org.uk/statistics-on-child-sexual-abuse/ [Accessed: 1 December 2015].

Travis, A. 2015. *Crime rate in England and Wales soars as cybercrime is included for first time* [Online]. Available at: http://www.theguardian.com/uk-news/2015/oct/15/rate-in-england-and-wales-soars-as-cybercrime-included-for-first-time [Accessed: 24 November 2015].

Wright, O. 2015. *George Osborne says Isis is planning to use cyber warfare to kill people in Britain* [Online]. Available at: http://www.independent.co.uk/news/uk/politics/paris-terror-attack-uk-government-to-invest-2bn-in-cyber-force-to-combat-online-terror-threats-a6737071.html [Accessed: 3 December 2015].