Computer Crime: Written Assignment

First Second Name

Institution of Affiliation

Computer Crime

Computer crime is fraud done online by professional computer users who hack other people’s or organization's confidential information and use them to access their financial accounts or other accounts. They may later steal from them these companies or individuals using the same computers (Great Britain, 2010).

To reduce these crimes, law enforcement officers should update laws on investigations that would lessen these crimes since it may not be easy to stop them completely. To do this, the law enforcement officers should prioritize the law of detaining anyone who is found to have committed cybercrime involving significant crimes like terrorism and bank robberies. This action would bring fear to anyone who thinks of using computers to commit terrorism, and he/she may avoid attempting such action. For other more minor crimes like hacking social media accounts, such offenses should block the victim from accessing the affected social media platform. This step will also create fear of hacking other people’s accounts by those who may think of attempting. The law enforcement officers can also encourage victims of such computer crimes to be reporting such actions. By registering these actions, law enforcement officers would present the cases to online platform developers. The developers will then trace how the crime was committed and develop measures to prevent a future repetition of similar crimes (International Telecommunication Union, 2014).

We should look at these crimes as illegal, no matter how small a crime seems to be. Crimes such as terrorism and bank robberies may result in the deaths of innocent citizens. (Great Britain, 2010). Crimes such as hacking of passwords of social media platforms may seem small, but they may lead to conflicts between individuals. For instance, if one hacks another's media platform and posts pictures related to a crime of murder, then the owner of this social media will be convicted in a court of law though he/she may be innocent. Governments need to modify their constitutions by setting stringent laws against these crimes. Governments may set rules of arresting anyone found attempting to do such crimes. They may also stop the operation of all organizations whose encryption of their online platforms is questionable, i.e., media that can easily leak their citizens' personal information. This law will protect the citizens from possible loss and leaking of their information to hackers.

References

International Telecommunication Union, (2014). *Understanding cybercrime: Phenomena, challenges, and legal response*

Great Britain. (2010). *Cybercrime strategy*. Norwich: TSO.