Cybercrime

[Enter your name here]

[Enter the name of the institution here]

The problem of cybercrime has come to the forefront of media ever since the internet went commercial and easily accessible to the general public. The main issues faced by legislators regarding these crimes are as follows:

These crimes do not fit into any of the major categories of the US law namely criminal, civil and regulatory laws. This makes it difficult for legislators to solve cases related to cybercrime. Similar issues are raised regarding the geographic vicinity in which the offence has been conducted. This creates problems for the investigators when the offender and the offended belong to different geographical areas. Even before considering the geographical area, it is very hard to know the identity of the person who has committed the crime in the first place. There are no specific courts or law enforcing agencies to adhere to these crimes.

These laws are designed to be reactive in nature because these laws respond to the actions taken by criminals. An example can be given when an additional firewall is developed after hacking of some official emails. If the organizations want to be safer in this regard, they have to adopt a proactive strategy which will implement safety precautions in advance.

Various websites should be accessible to only selected people who are from specific backgrounds. Instead of username and passwords, facial and biometric identifications can be used to access the websites.

The individuals should not provide any personal information on any unauthorized websites. This is especially true for the credit card and bank accounts information along with any personal pictures or videos... There should be a prompt report of any unusual activity on any website. Application of firewalls is also an option, especially where the connection is used by multiple people. In this case, all the users have to be assigned a specific user and password to log on.