NAME: UJEBE CHIOMA JOAN

DEPARTMENT: NURSING

MAT NO: 19/MHS02/118

COURSE CODE: GST122

 CYBER SECURITY

Cyber threats are evolving everyday thus increasing the need to develop and tighten security measures to ensure the protection of everyone using the cyber space. Increasing use of cyber space throughout the world coupled with globalization has increased the complexity of cyber threats. Cyber security threats continue to escalate in frequency and variation. This has led to major security threats thus the need for installation of better security measures to prevent the occurrence of these threats.

 The biggest nuisance and threat for the internet community of the world has to be hackers and spammers. Even the strongest security measures have not been able to contain this group of people. For instance, social sites like Facebook and twitter are sweet spots for hackers. However, the targets will probably be different because these unwanted cyber activities keep changing their platforms. They might now move to smartphones since most people now own them. Hackers also take advantage of results on search engines to spread malicious content.

There are also criminal groups which seek to extort money from the innocent and sometimes ignorant public. For instance, some of them will trick those using the internet into believing that they have won huge chunks of money. They will then ask them for bank accounts or credit card pin numbers. The moment they get information that they could use to access the users bank account, they make sure they drain their accounts. Alternatively some attack the system using spyware/malware so as to commit identity theft. There have been several cases where hackers would use email accounts of different people to extort money from their friends and relatives. For instance, the hacker will impersonate the owner of the email account and send messages to close friends asking them to send money to a specific account number on claims that the owner of the account might be in some kind of problem. So many people have fallen into such traps and lost so much money.

In order for the effects of cyber security threats to be reduced, the government has to put in place various measures to prevent such attacks. Its commendable that the government spends a lot of money to improve its private and public defenses against increasing aggressive and sophisticated foreign cyber threats. Individual users of the cyber space are vulnerable to cyber security threats because they lack the better awareness of the threats. As the attackers continue to aim at making more money, individual users become more vulnerable to bigger fraud and other financial damages. Most ignorant users are frequently lured by web site buttons and unknown mails and end up falling victim to phising and spyware. It is therefore important that the government comes up with a program where users of the cyber space are educated. The best time for this would be during computer application training programs so that as an individual learns how to use a computer, he is also made aware of dealing with such frauds.

Security seminars could also be established especially for cooperate users to help teach them on the awareness of cyber security threats and how to deal with them.

The government should invest more in improvement of software engineering and development. Cyber crime technology is also improving each and everyday. The colleges and universities should come up with curriculums that are intensive in teaching software engineering. Students from such courses will be very useful to the county’s security because they will be in a position to counter attack any threats from hackers to words the computer networks of important government institutions like the military and communication networks.

From the above discussion, it is evident that cyber security threats are very dangerous to the country’s security. The major problem has to be because technology is improving everyday and so are new ways for the hackers and cyber terrorists methods of breaching cyber security. It is good that there is common purpose around the world for reducing cyber security threats given the interdependent nature of the economies around the world and the connectivity of various communication systems. The private sector and the government should continue with building strong defensive capabilities as the enemies try to exploit vulnerabilities. However , defensive measures along are not enough. Given the persistent and evolving nature of cyber security threats, there is need to establish an international agreement for accountability, responsibility and deterrence in the frontier of digital warfare which is increasingly dangerous.