**CYBERCRIME AND THE ACADEMIC INSTITUTIONS NETWORKS (LAUTECH AS A CASE STUDY)**

**BY**

**ADEBAYO MODINAH GBEMISOLA**

**MATRIC NUMBER: 153302**

**BEGIN A PROJECT PROPOSAL SUBMITTED**

**TO**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING FACULTY OF ENGINEERING AND TECHNOLOGY, LADOKE AKINTOLA UNIVERSITY OF TECHNOLOGY OGBOMOSO, OYO STATE NIGERIA.**

**IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD BACHELOR OF TECHNOLOGY (B.TECH) DEGREE IN COMPUTER SCIENCE AND ENGINEERING**

**CHAPTER ONE**

**INTRODUCTION**

* 1. **Background of study**

It is obvious that the ICT meets a variety of educational, entertainment, communications, commerce needs, and other areas just few to mention, for its users. ‘With these benefits, though, this same technology has also ushered in a new wave of criminal activity called **cybercrime**’ (Saban, McGivern and Saykiewicz, 2002) defined as ‘any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime’ (Royal Canadian Mounted Police, 2000, in Hinduja and Schafer 2009) Cybercrimes are those crimes which are committed in the online or electronic environment.

The role that Information and Communication Technology (ICT) plays in all aspects of human endeavors is well documented and evident. ICT has integrated different economies of the world, through the aid of electronics via the internet. Many corporate organizations, including banks now depend on ICT and computer networks to perform basic as well as complex tasks. The electronic market is now open to everybody, including criminals. It is projected that by 2030, global Cyber security spending will reach $300bn, a 136% increase from $75bn in 2015.

As the Internet came into widespread commercial use, the nature of computer crimes began to shift. ‘While in some crimes, one component of the crime may have been committed using an electronic instrument, in other crimes, the crime as a whole is committed in the online or electronic environment. These crimes are also known as **cybercrimes**; generally occur in the virtual community of the Internet or in cyberspace’ (Heather 2008, Newton 2008).

Viruses, worms, hacking and Trojan horses are another serious threat. There is a variety of Cybercrime committed but these are the most prevalent and appear to be among the most troubling to computer users (Furnell, 2002 in Brett, 2008).

* 1. **Statement of problem**

The implications of cybercrime on international security have risen from the manner of technology use by individuals and a set of people known as cybercriminals. These people have mastered the art of computer networks to their advantage. Hidden behind computer monitors they commit atrocities such as data theft, hacking, espionage, and virus scattering. Most countries of the world have highly developed internet networks. Recently, there have been breakthroughs in the field as major telecommunication companies sprint to introduce 5G networks to the globe. However, there are fears that this network will also be used by criminals to gain access to victims organization network systems causing destruction and losses across all continents. Numerous techniques are being used by criminals of the 21st century to target sensitive data, recording the highest levels of fraud in history. At the hands of cybercriminals, victims lose private information, money, and even their characters. This study seeks to explore the forms of cybercrimes that have rocked the world in the new age. Additionally, the study seeks to examine the impact of such activities on academics institution network security and correspondingly, the measures to curb the situation academically.

* 1. **Aim and Objective**
     1. **Aim**

As cybercrime incidents are increase every day, the aim of this project is to reduce and eliminate cybercrime activities in the academic institutions network most especially in LAUTECH.

* + 1. **Objectives of the study**

1. To reduce the cybercrime activities in the academic institutions.
2. To introduce academic institutions to the various way of keep their data secure.
3. To create awareness for the academic institutions employee/staffs on the effect of linking of the organization information.
4. To introduce academic institution to various forms of cybercrimes adopted by cyber criminals in nowadays.
5. To discussing the major factors facilitating the rapid development of cybercrime in the academic institution.
6. To contribute appropriate measures to curb the growth of the cybercrime in the academic institutions.

* 1. **Significant of the study**

The study has the significance in observing the weaknesses present in the law governing cybercrime and strategic to initiate cybercrime law in academic institutions. Also identify the driving force succeed to solve that problem.

Therefore it provided challenges and suggests better recommendations to the government and academic institutions bodies to combat cybercrime.

* 1. **Scope of the study**

The study was to observe how academic institution combating a cybercrime. The research was interest to analyse the legal documents that can be used to stop computer crime. And what effort is taken to make academic institution and rest part of the world to be free from cybercrime. The study was focus on strategies that have been initiated by academic institutions to be free from cybercrime and make a digital life to be better place.