Chapter XV
Prevention of Cyber Crime in Cybercafés

Ogochukwu Thaddaeus Emiri
Delta State University, Nigeria

ABSTRACT

The purpose of this chapter is to examine the concept of cyber crime as it relates to cybercafés, forms of cyber crime, the role of the Internet, and suggest measures of cyber crime control and prevention in cybercafés. This chapter unveils the various forms of cyber crime and preventive measures with the view to addressing insecurity on the Internet and methods of protecting cybercafés systems. This chapter revealed some forms of cyber crimes to include computer viruses, data dwindling, hacking, data leakages, trapdoors, scavenging, e-mail bombing, and so forth, and equally suggested preventive measures such as user education, legal regulations against cyber crimes, international cooperation, restricting system use, limiting access to certain programs, and so forth.

INTRODUCTION

The advent of the Internet has transformed the way we communicate, educate, and sell goods and services. Without doubt, the *Internet* is fast altering the processes and nature of conducting human activities, be it business, politics, administration, education, social, or religion. The *Internet* has made changes in almost all aspects of our lives as it plays a role in most of what we discuss today about access to dissemination and retrieval of information (Chachage, 2001).

According to Paul (2002), the *Internet*, which began in the 1960's as a project of few researchers, has grown to be a commercial success with billions of dollars of annual investment; it has developed within three decades into a mass medium that influences most or all domains of

life: from education to recreation; from business to medicine, and from academia to politics. He notes further that influence of the Internet permeates all aspects of life-in developing as well as developed counties.

The use of *Internet* has grown tremendously across the world. This growth as put by Jensen (2002) could be the reason for the growing number of cybercafés, which enables people to have access to the Internet. The 2002 status report on the state of Internet connectivity indicated that as of mid-2002 the number of dial-up Internet subscribers was close to 1.7 million, even in Africa, 20% up from the present year, mainly bolstered by growth in a few of the larger countries such as Egypt, South Africa, Morocco, and Nigeria, that shared public access and use of corporate networks is continuing to grow at greater rate than the number of dial-up users (Adomi, Okiy, & Ruteyan, 2003). According to them, the report further notes that there are now many thousands of cybercafés/business centres in the major cities of such African countries, run by small entrepreneurs who are allowed by the regulator to provide VOIP services as part of their cybercafé licence, which cost about $500 a year.

As the use of *Internet* is greatly increasing, so also criminal activities are increasing. Datal (2006) observed that information technology is a double-edged sword, which can be used for destructive purposes as well as constructive work. This chapter will attempt to look at what cyber crimes are, the various forms of cyber crimes, the role of the Internet, how cyber crimes are perpetuated, and prevented and controlled in cybercafés.

BACKGROUND

Adomi et al. (2003) defined *cybercafés* as a place where public Internet access is provided by entrepreneurs for a fee. They are place where people can have access to computers that are connected to the Internet and pay a token amount for using them (Adomi, Omodako, & Otolo, 2004). *Cybercafés* are places where people with little fees can access the superhighway of information on the Internet.

Adomi, Omodako, and Otolo (2004) opined that in the USA the term *cybercafés* often refer to true cafés offering both Internet access and beverages, in Nigeria and other parts of Africa, cybercafés can be referred to as places offering public Internet access in places like restaurants or hostels or they could be places that are wholly set aside for public access Internet services.

Wirsiy and Shafack (2002) assert that allowing people public access to *Internet* services at tolerable prices has made it possible for individuals everywhere with a personal computer and functional telephone to have access to millions of pages of information. According to them, this is the greatest impact of this new technology because of narrowing the gap between the information haves and have-nots, which was exacerbated during the print-media-based information resources was very expensive and thus increased the gap, as recessions and other catastrophes like drought famine, hurricanes, flood, wars, and other conflicts continued to tall tolls on developing counties, especially those in sub-Saharan Africa. In spite of these obvious advantages of the Internet, extensive use has created new problems that must be dealt with. Just as the computers success is attributed to people's imagination, many of the problematic situations that must be dealt with result from human nature. One of such crucial issues is cyber crime.

Cyber crime implies a wide variety of criminal offence, activities, or issues in the Internet or in cybercafés. Broadly, the term cyber crimes are computer related crimes. However, some others distinguish between *cyber crimes* and computer crimes. Nomokonov (2003) opined that *cyber crimes* present a common concept embracing computer crimes in a narrow sense, that is, where a computer is an object whereas information se-