Chapter XII
Computer Virus Phenomena in Cybercafé

Abdul Rahman Garuba
University of Benin, Nigeria

ABSTRACT

The chapter examines the concepts, history, sources, spread, detection, and removal of computer viruses. The increase in the number of computers and accessibility to Internet has made it easy for hackers to invade systems all over the world. Computer viruses have reached epidemic numbers in many computer environments resulting in computer security vulnerabilities. Cybercafés systems/networks are potential objects of virus attacks due to the fact that they are connected to the Net. Cybercafé managers should have a good understanding of the risk and controls associated with various security technologies. It is the hope of the author that adequate awareness and understanding of the destructive devices by cybercafé managers and computer users generally will help secure their systems. It is recommended that cybercafé administrators develop a security policy for both employees and users.

INTRODUCTION

The introduction of microcomputers has forever changed the ways we do things and has led to the proliferation of computer networks worldwide. The Internet has thus become an incredible means for information, communication, and human networking. Although information and communication technology (ICT) first imparted in Nigeria in the 1950s (Longe & Longe, 2005), it was the promulgation of the Nigerian Information Technology Development Agency (NITDA) Act in 2007 that the Internet began to penetrate Nigeria (Akwaja, 2007). The introduction of cybercafés in the major cities of Nigeria is a deliberate attempt to enable more users to have access to the Internet for research, academics, and business. A status report on the African continent cited by

Adomi, Okiy, and Ruteyan (2003) confirm that the proliferation of cybercafés and business centers in the major cities of Nigeria have enabled rural dwellers to have access to the Internet. Research also shows that 60% of Internet use is devoted to information on academics, entertainment migration, sports, and 40% is devoted to pornography (Longe & Longe, 2005). Pornography is a means used by virus writers to trick innocent viewers to download potential dangerous *Trojan horses*.

The proliferation of the cybercafés comes with security threats from viruses. The cybercafés users are thus faced with these destructive devices which they unknowingly introduce to the computers mostly from e-mail attachments and other adult sites. These devices used to circumvent computer security in cybercafés are viruses, worms, Trojan horses, and other malicious codes such as spyware and adware (Argaez, 2007). Cha (2005) noted that hackers, viruses, worms, spyware, and phishing sites have proliferated the Internet to the point where it is nearly impossible for most computer users to go online without falling victim to them. These devices are hidden within programs or attached to e-mail. These programs, except with few, require human intervention to activate. In other words, a user must deliberately run the infected program before it can cause damage. While the benign ones only makes copies of themselves and continue spreading, the most dangerous can randomly e-mail confidential information, destroy all the data on your disk drive, or even give complete access to your computer connected to the Internet (Nepil, 2003). The old saying that what you do not know cannot hurt you may not be true as far as computer viruses are concerned. As long as you are connected to the Internet, anything can happen, your computer can be cracked and a virus or worm introduced into the computer. In Nigeria, education and awareness about security is largely poor and this could provide a safe haven for break in. Most individual Internet users therefore require adequate computer virus education.

As more Nigerians users turn to the use of the Internet, more computers whether personal, corporate, or government, the warfare will increase unless users have a minimum know how of how to recognize and prevent virus attacks using virus techniques.

This chapter will address the issues such as: what are viruses, worms, and Trojans; their origin and creations and why; methods of spreading in cybercafés, detection, and their removal. The overall aim being that of educating and creating awareness about the destructive capabilities of viruses and thereby proving the much needed virus security education. In conclusion, this chapter is intended to educate both the causal and technical Internet user to possible risks posed by virus and viruses, thereby providing them the key to know how to recognize a virus attack and dispel the myth surrounding viruses.

BACKGROUND

The phenomenon of the computer virus has today become one of the most interesting moments of the 20th century's technical progress (Kaspersky, 2006). Computer viruses have caused serious problems that in 1998 William H. Gates, Chairman of Microsoft acknowledged that the plaque of viruses and worms afflicting Windows and other products had gotten out of hand and needed drastic measure (Hamm, 2006). With the increase in the number of computer users over the last 30 years, some groups of persons decided to develop programs that would make the computer malfunction. Because of the rate at which computer users, including organizations, have lost important data and hard disks, there has been call to fight the scourge (INTECU, 2006). The "I love you" virus for example, is said to have caused over $1 billion in lost productivity when it crippled e-mail systems world wide. In 2006, it was reported in learn the Net (2006) that 10,000