UNIT 18 Data Security 1

INTRODUCTION

There are a variety of different crimes that can be committed in computing, including:

Computer Crime	Description
Spreading viruses	distributing programs that can reproduce themselves and are written with the purpose of causing damage or causing a computer to behave in an unusual way
Hacking	gaining unauthorised access to a network system
Salami shaving	manipulating programs or data so that small amounts of money are deducted from a large number of transactions or accounts and accumulated elsewhere.The victims are often unaware of the crime because the amount taken from any individual is so small.
Denial of service attack	swamping a server with large numbers of requests
Trojan horse	a technique that involves adding concealed instructions to a computer program so that it will still work but will also perform prohibited duties. In other words, it appears to do something useful but actually does something destructive in the background.
Trapdoors	a technique that involves leaving, within a completed program, an illicit program that allows unauthorised – and unknown – entry
Mail bombing	inundating an email address with thousands of messages, slowing or even crashing the server
Software piracy	unauthorised copying of a program for sale or distributing to other users
Piggybacking	using another person's identification code or using that person's files before he or she has **logged off** (disconnected from a network account)
Spoofing	tricking a user into revealing confidential information such as an access code or a credit-card number
Defacing	changing the information shown on another person's website
Hijacking	redirecting anyone trying to visit a certain site elsewhere

A **computer virus** is a program that can reproduce itself and is written with the purpose of causing damage or causing a computer to behave in an unusual way. It **infects** other programs i.e. it attaches itself to other programs, known as **host programs,** and therefore reproduces itself. It operates by replacing the first instruction in the host program with a **JUMP command.** This is a command that changes the normal instruction sequence in a program, causing the virus instructions to be **executed** (processed by the processor) before the host program instructions. When the virus has been executed, the host program is executed in the normal way.

When it attaches to operating system programs to integrate itself with the operating system (the set of programs that control the basic functions of a computer and provide communication between the applications programs and the hardware), it is said to have

patched the operating system. Viruses normally attach themselves to programs that have a COM extension (e.g. command.com) that are known as command files or **COM files**, or to programs that have an EXE extension (e.g. explorer.exe) that are known as executable files or **EXE files**. A virus is **loaded** into memory (copied from the storage media into memory) when a program it has attached itself to is **run** or **executed** (processed by the processor). It then becomes **memory resident** i.e. it stays in the memory until the computer is switched off. When the virus is **triggered** by a predetermined event, it operates the **payload** (the part of the virus that causes the damage). Although a virus is the term used to describe any program that can reproduce itself, viruses usually have four main parts:

a a **misdirection routine** that enables it to hide itself

b a **reproduction routine** that allows it to copy itself to other programs

c a **trigger** that causes the payload to be activated at a particular time or when a particular event takes place

d a **payload** that may be a fairly harmless joke or may be very destructive.

A program that has a payload but does not have a reproduction routine is known as a **Trojan**. Each virus is given a name e.g. Love Bug and can be classified as a particular type of virus. Virus types include: **logic bombs** that destroy data when triggered; **boot sector viruses** that store themselves in the **boot sector** of a disk (the part of a disk containing the programs used to start up a computer); **file viruses** that attach themselves to COM files; **macro viruses** that are small macro programs that attach themselves to wordprocessor files and use the macro programming facilities provided in some wordprocessor programs.

OBJECTIVES

By the end of this unit, Ss should be better at:

- scanning a text, ignoring irrelevant information
- inferring information from a reading text
- exchanging information orally
- writing a description of a computer crime.

They should understand and be able to use:

- ways to link cause and effect relationships
- *en-/-en* verbs.

They should know and be able to use terms associated with Data Security such as: *defacing, denial of service attack, hijacking, mail bombing, piggybacking, salami shaving, software piracy, spoofing, trapdoors, trojan horse, viruses.*

STARTER

1 and **2** Do these in small groups. If you have access to English language newspapers, look out for other headlines like these to use with your students. *Scam* here means a plan to cheat people of money.

Key 1

1 Damaging effects of the love bug virus.
2 Illegal hacking into Microsoft's software codes.
3 Scheme to make money illegally using Web phones.

Key 2

Refer back to these lists when doing Task 8. In addition note *data diddling*, feeding false data into a computer.