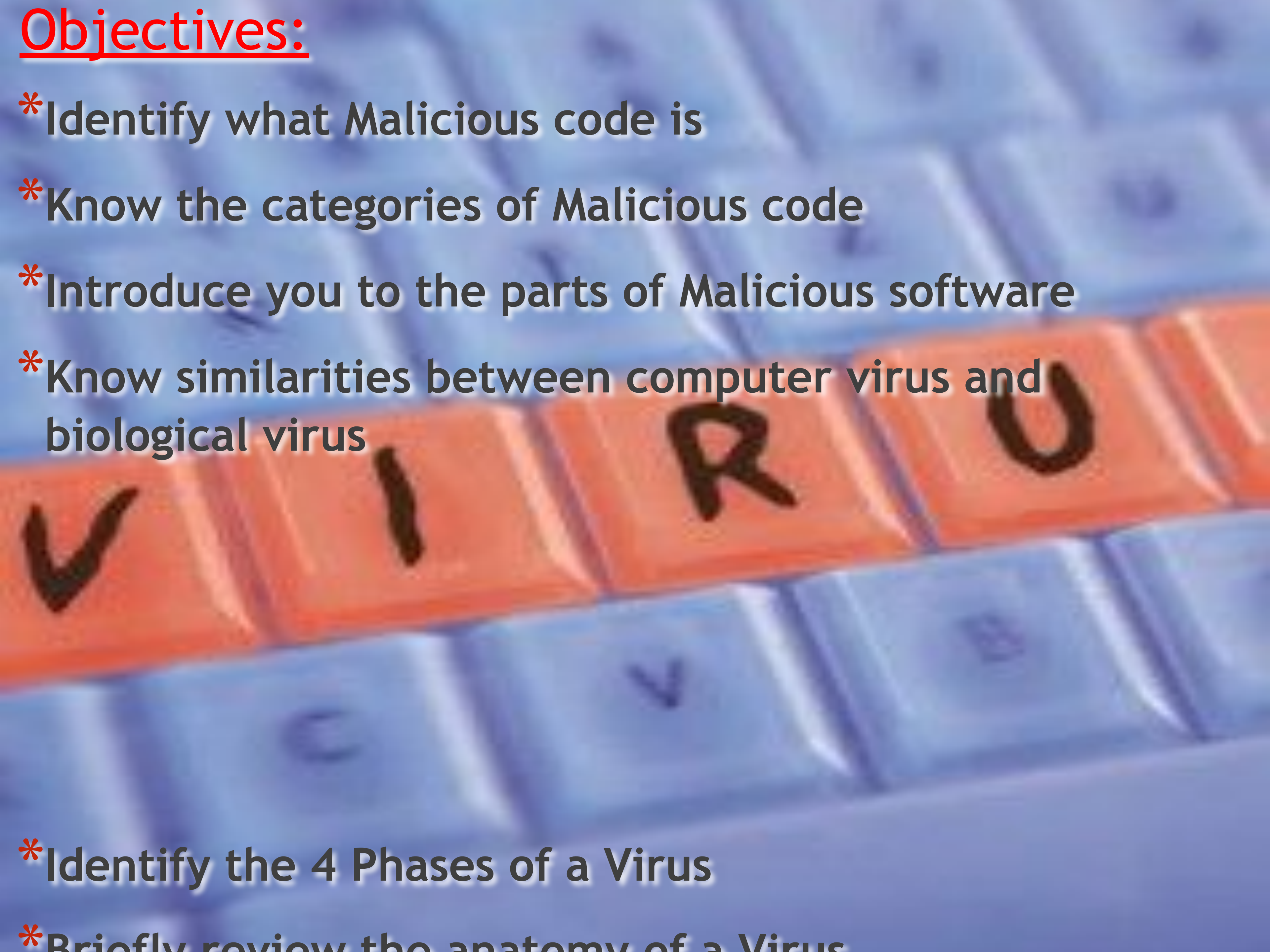
Malicious Code

Objectives:

- Identify what Malicious code is
- Know the categories of Malicious code
- Introduce you to the parts of Malicious software
- Know similarities between computer virus and biological virus



- Identify the 4 Phases of a Virus
- Briefly review the anatomy of a Virus

What is malicious code?

A broad category of software threats to your network and systems

- Modifies or destroys data
- Steals data
- Allows unauthorized access,
- Exploits or damages a system

A Computer Program is designed to achieve a particular function

Malicious when the designed to cause adverse effects

AKA: Programmed Threats

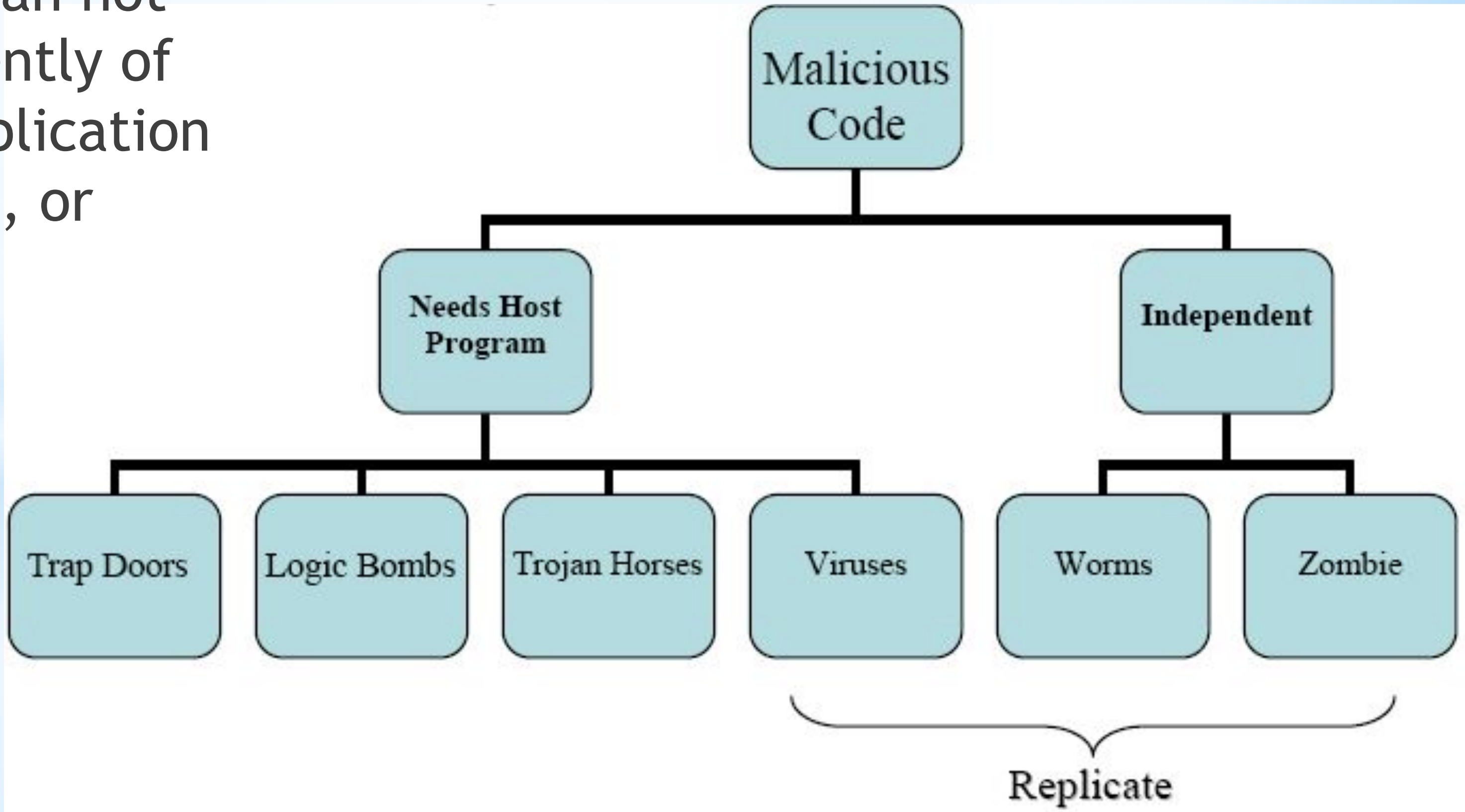
Two categories of Malicious Code

Independent:

Self contained program that can be scheduled and ran by the operating system

Needs Host Program:

essential fragments of programs that can not exist independently of some actual application program, utility, or system program

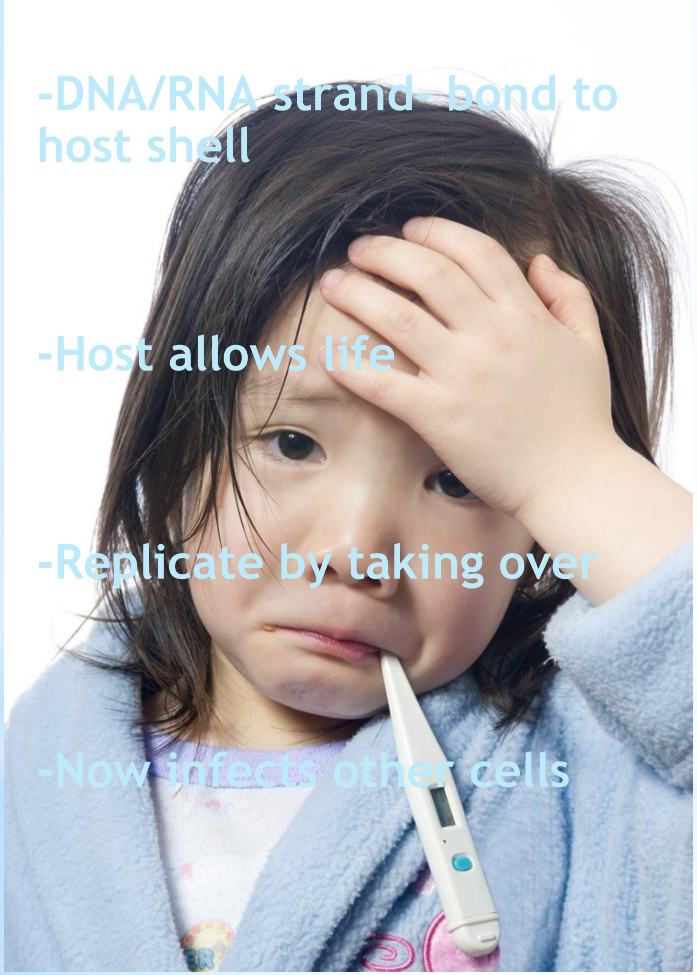


Parts Of Malicious Software

- Trap Doors: Secret entry
- Logic Bombs: code embedded in a program
- Trojan Horses: security breaking program
- Zombies: takes over another internet- attached computer
- Viruses: Infects other programs

Biological Virus VS. Computer Virus

Biological



-DNA/RNA strand- bond to host shell

-Host allows life

-Replicate by taking over

-Now infects other cells

Computer

-Instructions stored in host program

-Active when host is executed

-Replicate when host program is executed

Now infects other programs

Four Phases of a Virus

1. Dormant Phase

2. Propagation Phase

3. Triggering Phase

4. Execution Phase

Virus Structure has four ports

1- Mark can prevent re-infection attempts

2- Infection Mechanism causes spread to other files

3- Trigger are conditions for delivering payload

4- Payload is the possible damage to infected computer