Introduction to Computer Virus and Malware

Introduction

Presentation Content

- Description
- Virus Characteristics
- Different Types of Malwares
- Different Types of Viruses
- Safe Computing Tips and Techniques

Description

What is a Computer Virus?

A program (a block of executable code) that has the ability to replicate, or make copies of itself, and spread to other files.

Description

What is a Malware?

Unexpected or malicious program or mobile codes

What does a Malware do to a Computer

Some Possible Malware Payloads:

- Simple display of messages
- Delete or corrupt files,hard disk
- Interfere with computer operations
- Spread to other files and computers
- Compromise computer or network security

How do Viruses and Other Malware spread?

They spread…

From Disk to Disk

From Program to Program

From Document to Document

Via E-mail and Internet

Over the Network

Virus Characteristics

Virus Characteristics

Direct-Action vs. Memory-Resident

Direct-Action

Infect files during execution of virus

Memory-Resident

- Installs itself in memory
- Monitors the activity of the computer
- Infects files on certain conditions

(i.e. when they are executed, opened, etc.)

Virus Characteristics

Stealth

Implements a way to hide modifications

Polymorphic

Produces varied but functional copies of itself.

Different Forms of Malware

Different Types of Malwares

- Viruses

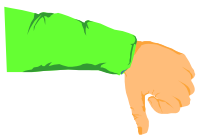
- Trojans

- Worms

- Joke Programs

- Droppers

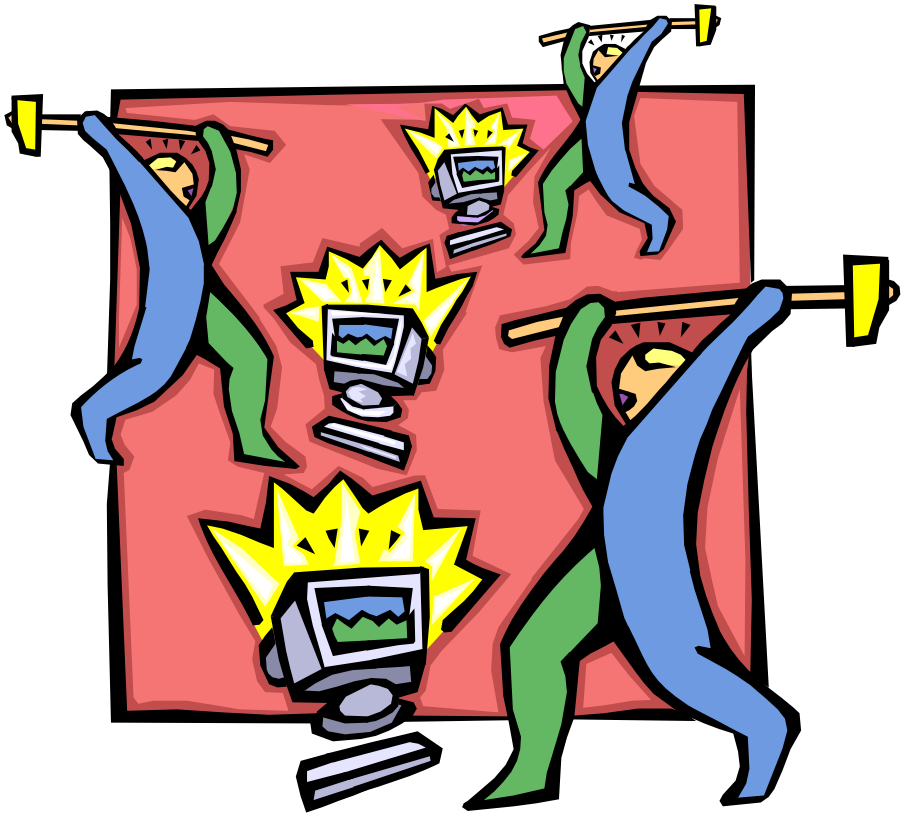
- Backdoors



- DDos Programs

Trojan Programs

Trojan Horse Programs



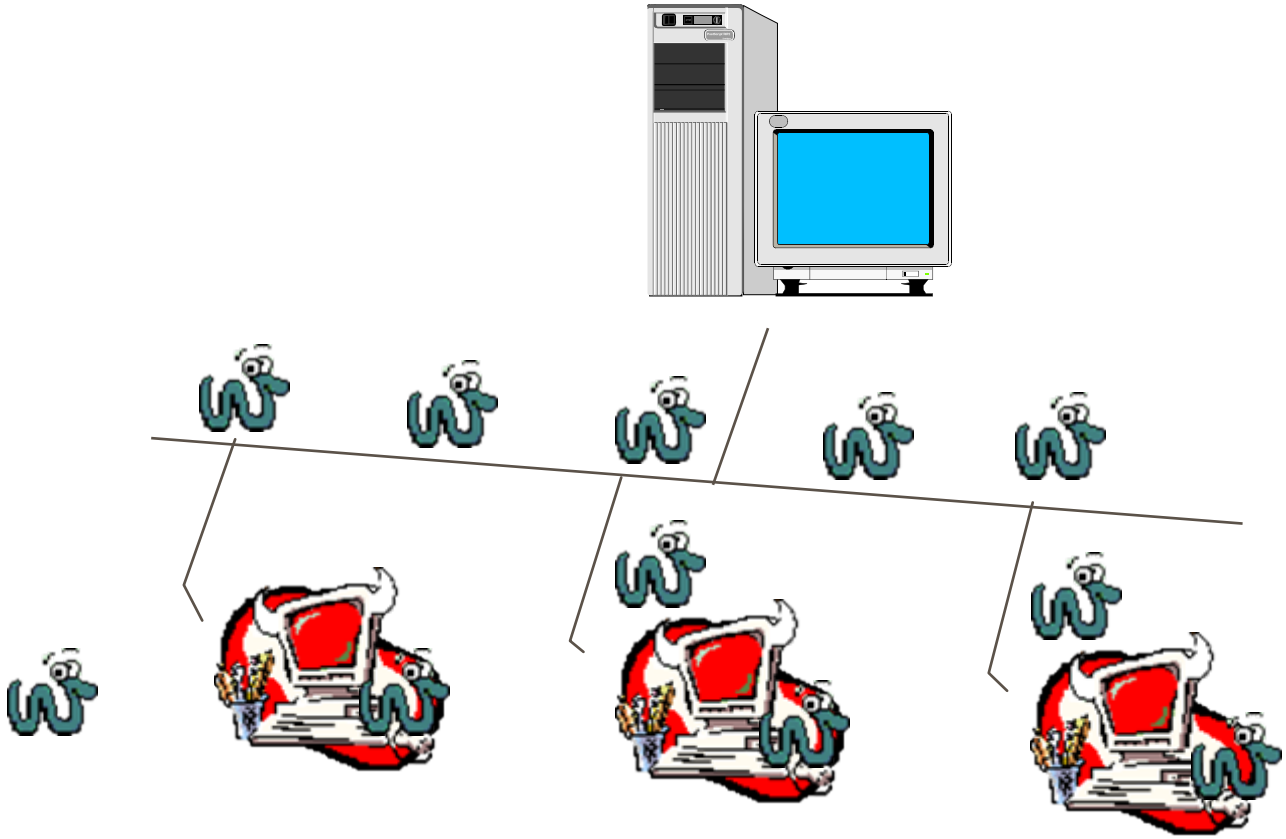
Trojans are programs that may appear harmless, but perform unexpected or unauthorized, usually malicious, actions

The Dangers of a Trojan

- downloading and uploading files on their computer
- reading all of their IRC logs and learning interesting things about them and their friends.
- reading their ICQ messages.
- stealing information such as credit card numbers, username and passwords, etc..
- and worst…deleting their files, formatting their hard drive.

Computer Worms

Worms



A computer worm is a program (or set of programs) that is able to spread copies of itself to other computer systems.Unlike viruses, worms do not need to attach themselves to host programs.

Checking for Trojans and Worms

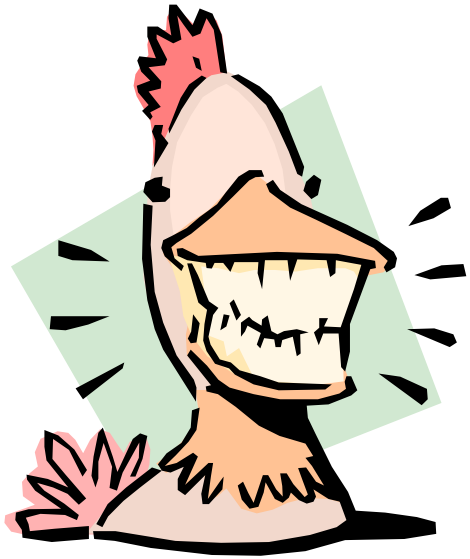
Some Symptoms:

- Unusual system slowdown and/or behavior
- Unusual tasks running
- Modifications on the Registry
- Modifications in configuration files.
- Unusual emails sent
  (without the user’s consent)

Joke Programs

Joke Programs

- Ordinary executable programs.
- Created to make fun of users.
- These programs do not intend to destroy data



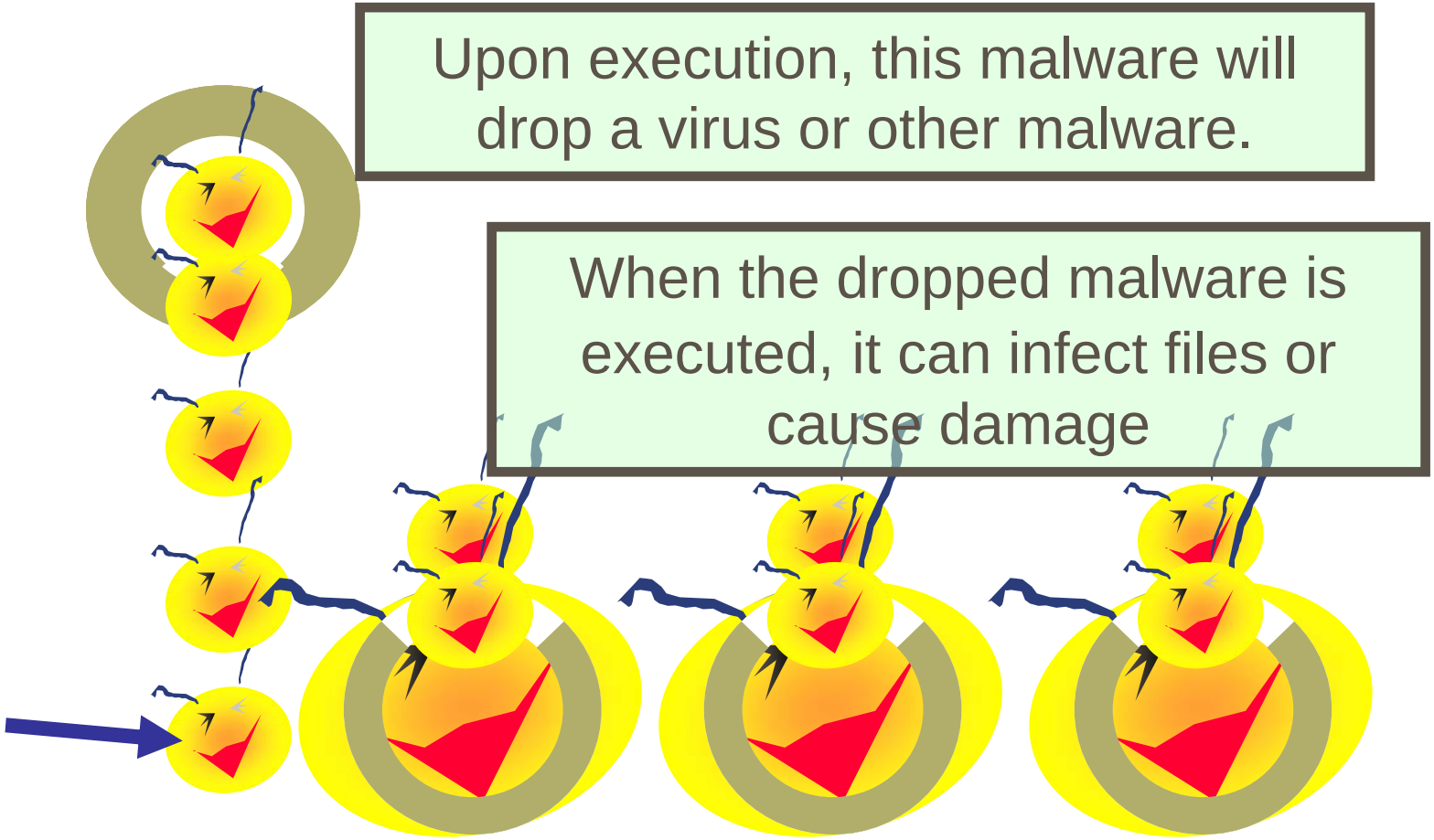
Joke Programs

Some Characteristics:

- Similar to ordinary executable programs
- Will not infect other programs
- Will not do any damage directly
- May annoy or tease the user
- May be difficult to halt or terminate
- May cause some devices (e.g., mouse or keyboard) to temporarily function abnormally

Malware Droppers

Malware Droppers



A program that drops a virus or other malware

Backdoors

Backdoors

A backdoor is a program that opens secret access to systems, and is often used to bypass system security.

Backdoors

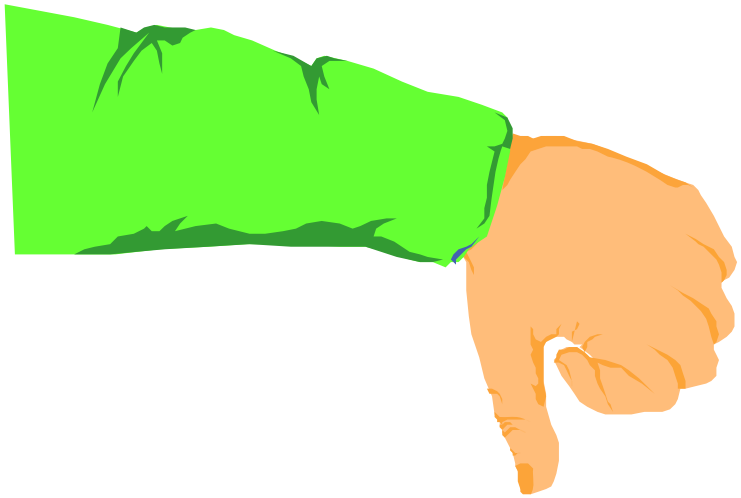
Here are some of the things that these backdoors are capable of:

- Log keystrokes
- Edit or delete files and folders
- Edit the registry
- Send out confidential information such as password to the hacker
- Run programs on the host or target machine
- Restart or shut down the computer
- Capture screens
- Browse and send out files to the hacker
- Change computer settings such as wallpaper
- Kill or disable running programs

DDos Programs

DDoS Programs

DDoS programs are made by attackers to disable web servers, thereby preventing legitimate users from using their services.



DDos stands for Distributed Denial of Service

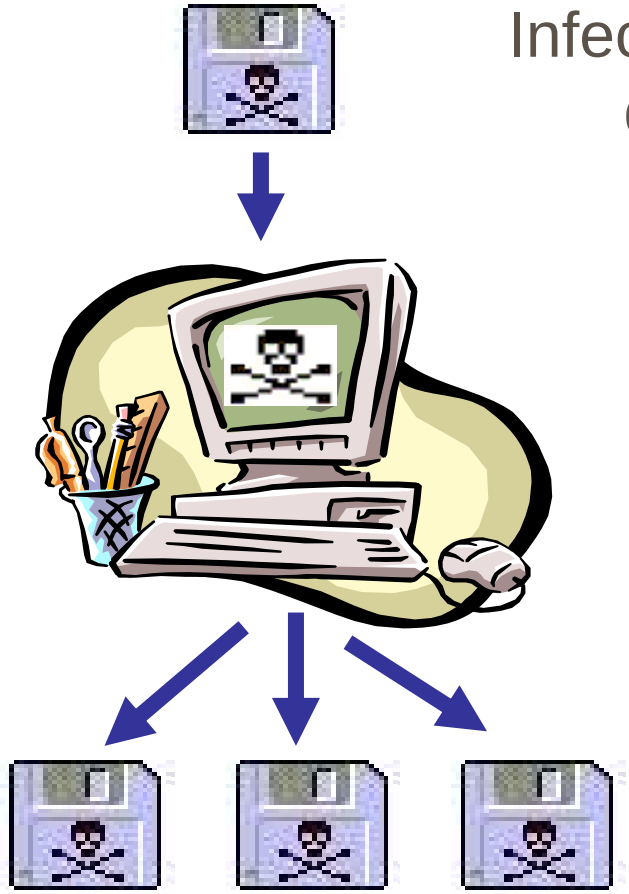
Different Types of Viruses

Classification of Viruses

- Boot Viruses 
- DOS Viruses 
- Windows Viruses 
- Script Viruses 
- Macro Viruses 

Boot Viruses

Boot Viruses



Infected diskette used during bootup

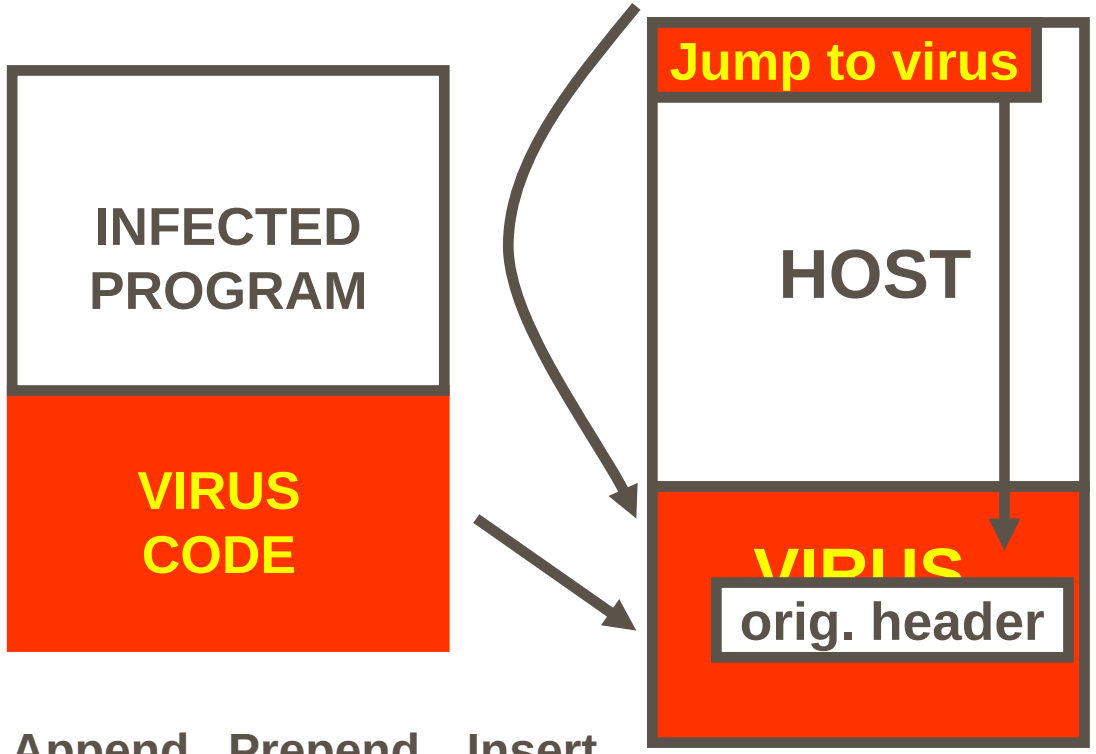
Boot virus infects the hard disk

Every disk used afterwards is also infected

DOS Viruses

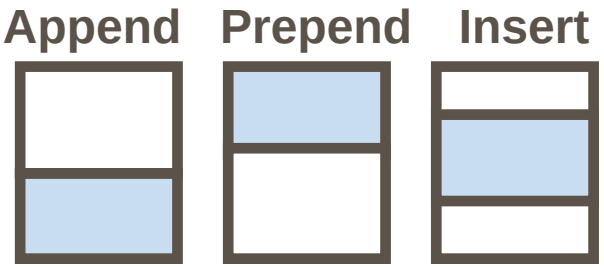
DOS Viruses

A virus usually infects by attaching a copy of itself at the tail of the host program.



Then, it saves a copy of the original header somewhere in the virus body

It modifies the header to gain control when the program executes.



Although most viruses append their codes, some also prepend, insert, or overwrite their virus codes.

DOS Viruses

Some symptoms

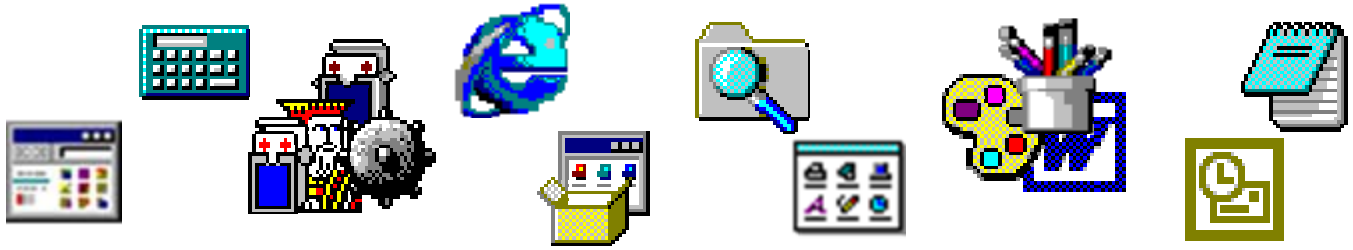
- increase in the file size of infected programs
- decrease in the size of available memory
- unusual slowdown of computer system

Windows Viruses

Windows Viruses

Commonly infected file types:

- Applications/executable files (*.EXE)



- Device drivers (*.DLL, *.DRV, *.VXD)

- Other file types with executable codes (*.SCR, *.HLP, *.OCX)

Windows Viruses

Things to check:

- **Unnecessary changes in executable files (i.e.: file size, timestamp, behavior, etc.)**
- **Any unusual tasks/processes**
- **The Registry and other configuration files for any unusual or suspicious modifications**

Macro Viruses

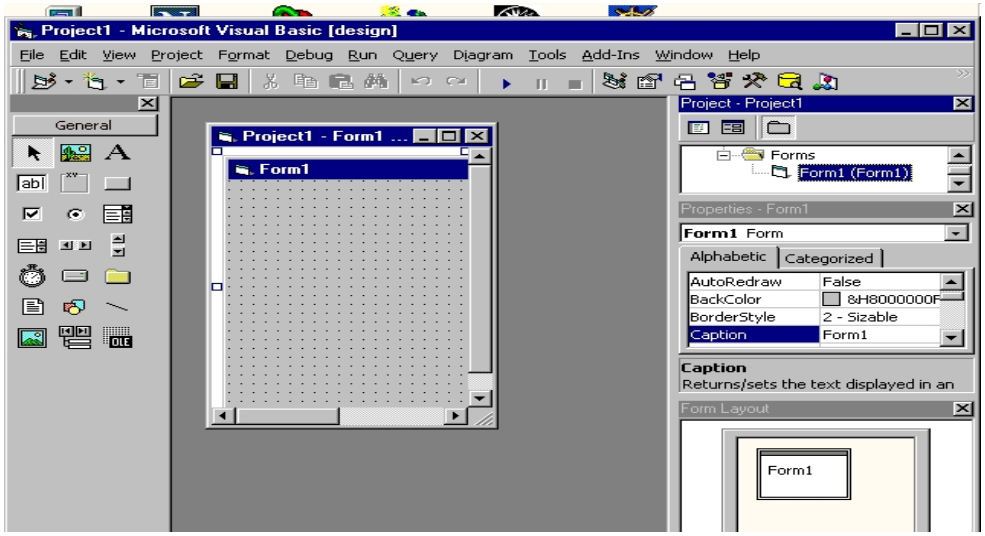
What is a Macro?

Collection of instructions

Handles boring, awkward, and tedious tasks

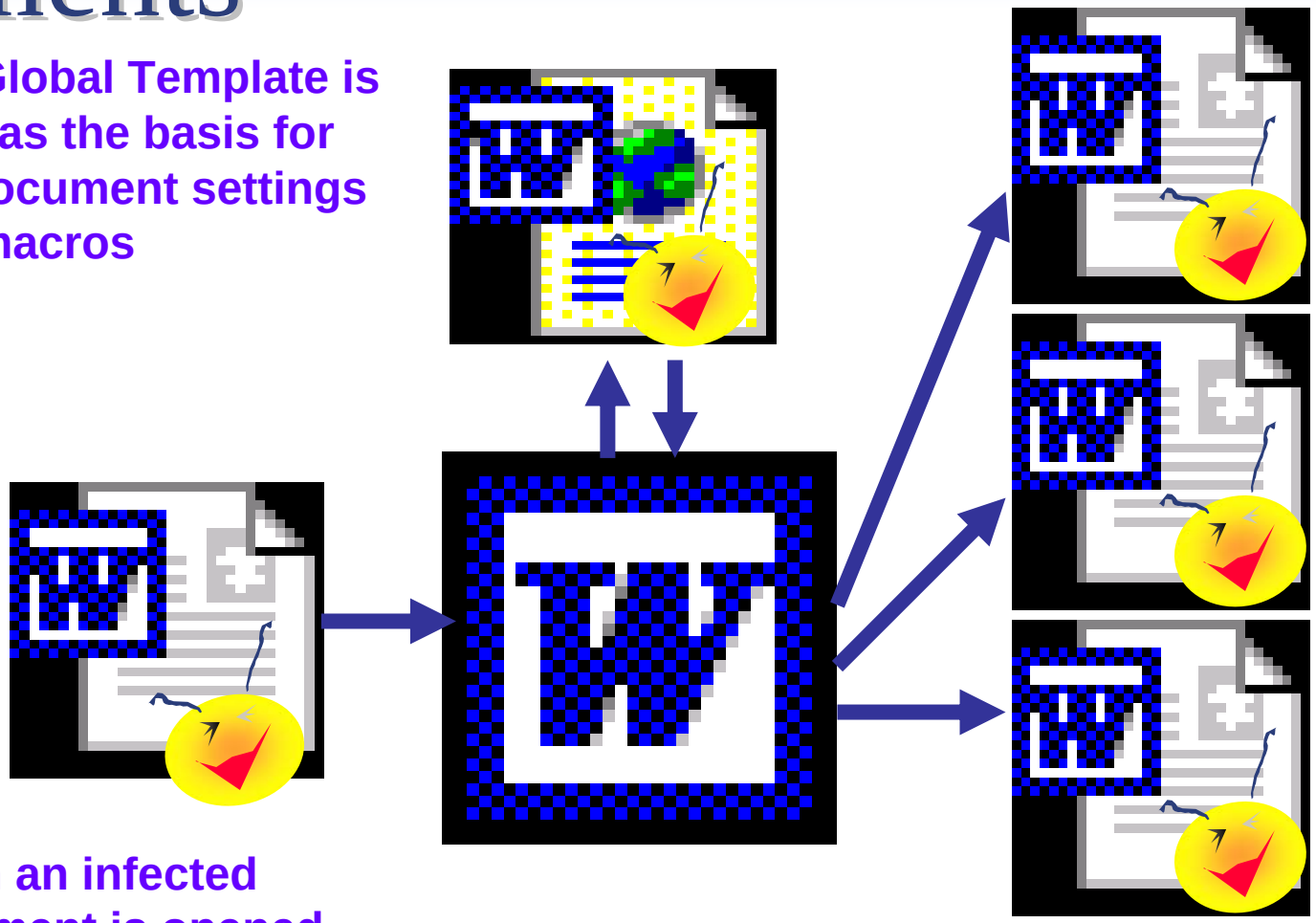
Saves a user keystrokes.

Visual Basic® for Applications (VBA) Environment



Macro Viruses in Word Documents

The Global Template is used as the basis for the document settings and macros

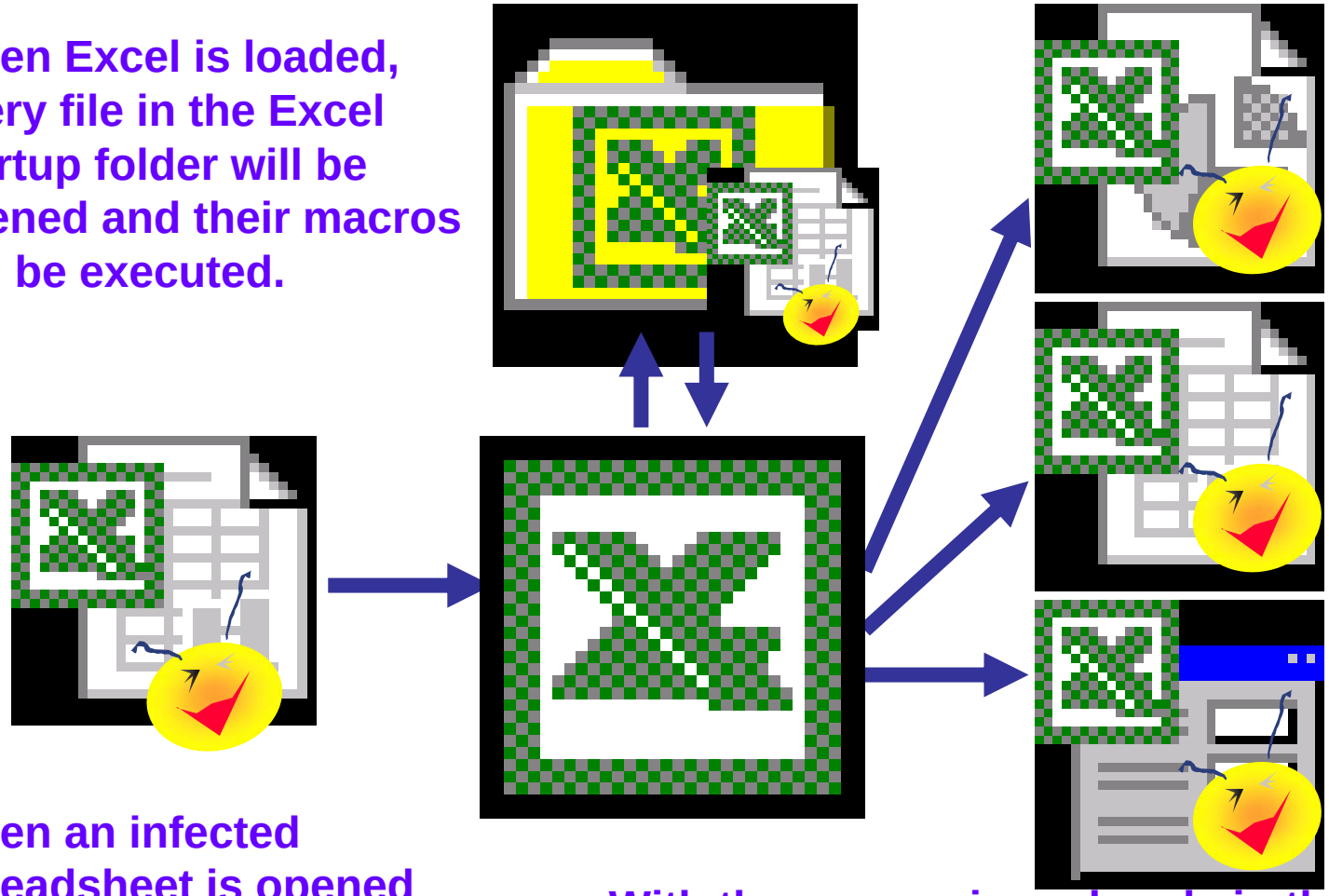


When an infected document is opened with Word, it will usually copy its macro codes in the Global Template

With the macro virus already resident in the Global Template, it can already produce additional copies of itself to other documents accessed by Word.

Macro Viruses in Excel Documents

When Excel is loaded, every file in the Excel startup folder will be opened and their macros will be executed.

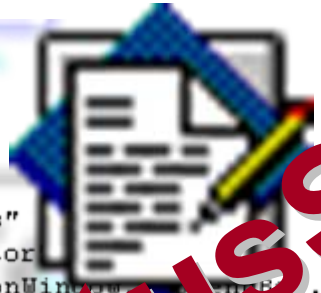


When an infected spreadsheet is opened with Excel, it will usually drop a copy of itself unto the startup folder.

With the macro virus already in the startup folder, it can already produce additional copies of itself to other spreadsheets accessed by Excel.

Macro Viruses in other file types

```
Sub Main()
    Key% = Asc("S")
    alt = &H2000

    'get the menuid
    mainMenu = "&Edit"
    Item1 = "Scr&ipt && Macros"
    Item2 = "Show Script &Editor
    Set mainMenu = .ApplicationWin                .Items.Item(mainMenu)
    Set Item = mainMenu.Items.Item
    ItemId = Item.ID

    'define the persisten  acce    tor key A                 the script editor
    .ApplicationWindow.Acc    tors.AddAccel                 + alt, ItemId, 0
End Sub

Sub Opened(Source As Document)
  Dim EditMenu As Menu
  Set EditMenu = CurrentApplication.CurrentMenuBar.GetMenu(2)
  EditMenu.AddItem -1, "&Payro          "Perform payroll calculati                alc"
End Sub

Sub Pay
  Me                el      c."
End

Sub Cli                Button)
    D                 New NotesUIWorkspace
    Di          NotesUIDocument
    Dim sheet As Variant
    Set uidoc = workspace.CurrentDo      ment
    uidoc.EditMode = True
    Set sheet = uidoc.GetObject("spre
    sheet.ranges.Item("A1").contents = "Howdy"
End Sub
```



LotusScript

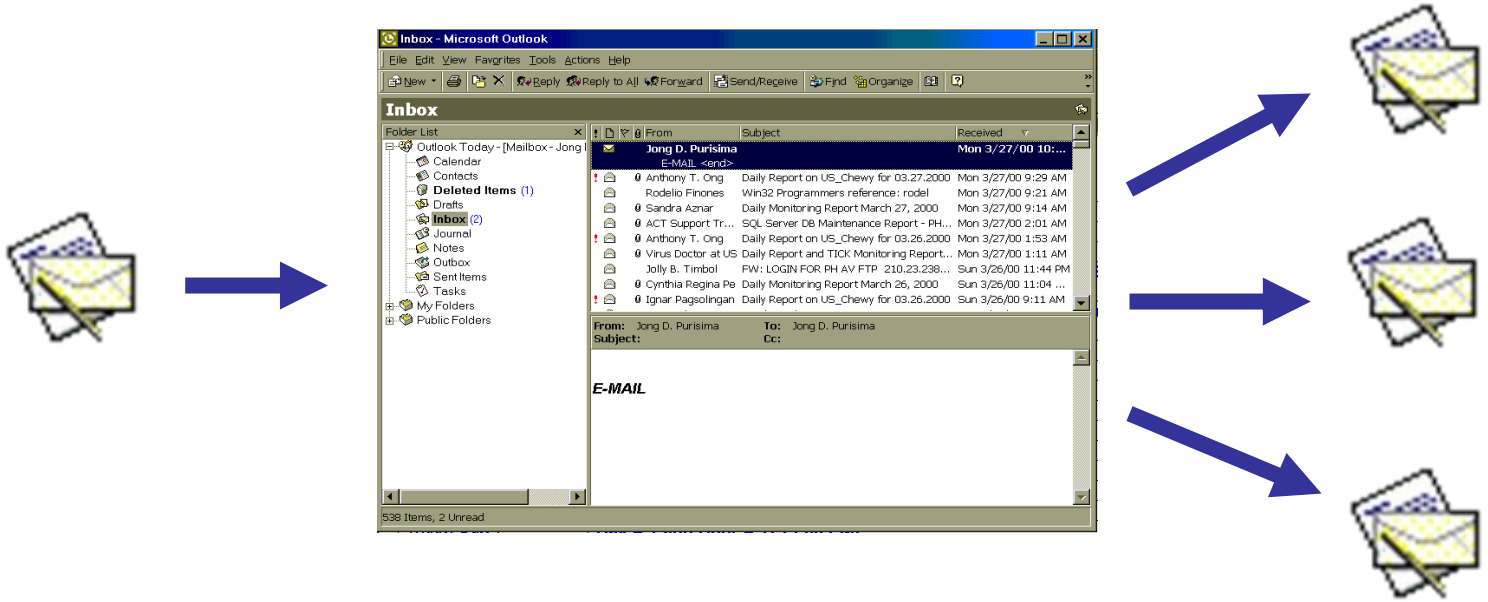
VBA

CorelScript

Script Viruses

If a mail message or a Web page has some malicious scripts

the malicious scripts may utilize the scripting host execution capabilities of some Web and mail browsers



thus enabling them to spread and replicate to other mail recipients or Web page users

Safety Computing
Tips and Techniques

Safe Computing Tips & Techniques

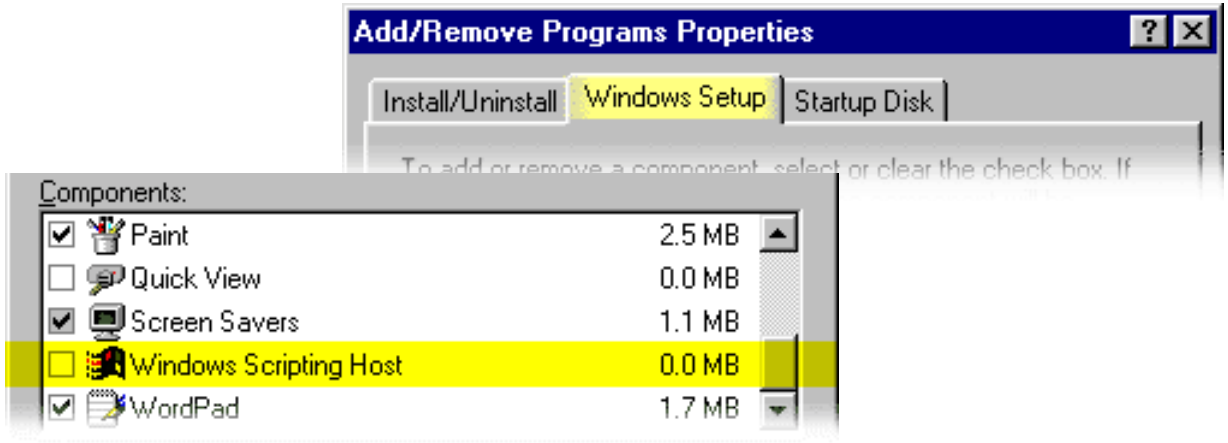
1. **Disable the Windows Scripting Host functionality**
2. **Do not hide the file extensions of known file types**
3. **Set up the Internet Explorer security setting**
4. **Apply the latest Microsoft security updates**
5. **Enabling Macro Virus Protection**
6. **Scan floppy diskettes before use**
7. **Enable Virus Warning in CMOS setup**

Safe Computing Tips & Techniques

Disable the Windows Scripting Host functionality

This prevents Visual Basic script viruses and malware from running, so that they cannot activate, spread or cause damage to files.

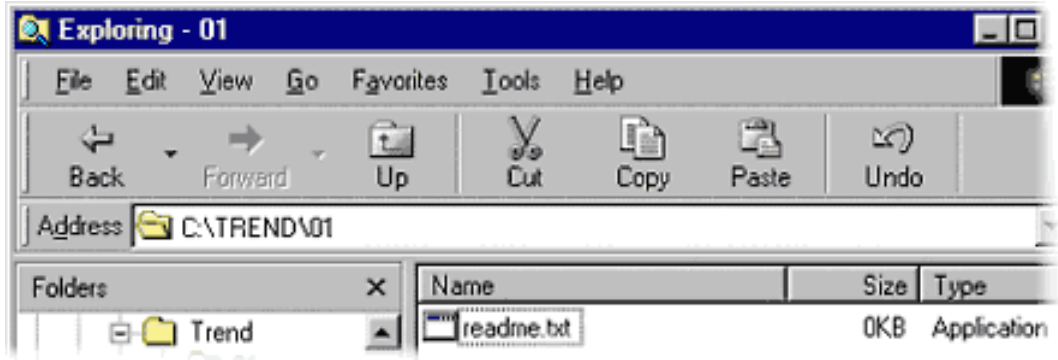
A typical PC does not need Windows Scripting Host (WSH) to function normally. Therefore, it is usually ok to disable it. You can always reinstall WSH if you change your mind later.



Safe Computing Tips & Techniques

Do not hide the file extensions of known file types

All Windows operating systems, by default, hide the known file extensions in Windows Explorer. This feature can be used by virus writers and hackers to disguise malicious programs as some other file formats, such as text, video or audio files.

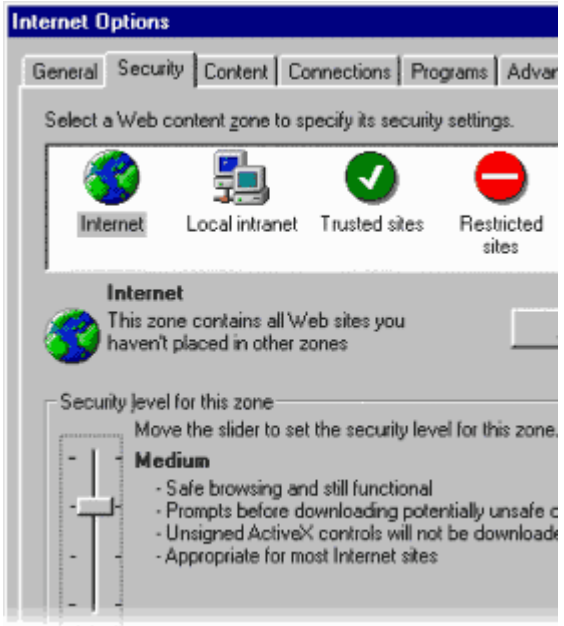


Safe Computing Tips & Techniques

Set up the Internet Explorer security setting to Medium or High

By default, the Internet Explorer security setting is set to "Medium." However, some viruses and malware have been found to have the ability to change the settings to "Low" and therefore allowing the system to be vulnerable.

It is encouraged that the security setting is set to at least "Medium" to reduce the risk of accidentally running a malicious file. At the "Medium" security level, Internet Explorer will prompt the user before running a potentially unsafe content.

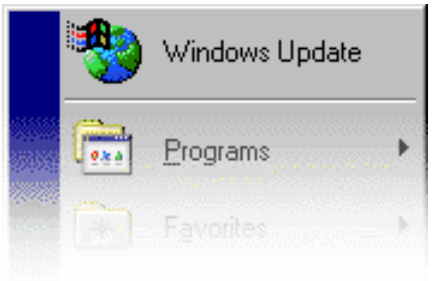


Safe Computing Tips & Techniques

Apply the latest Microsoft security updates

Security updates will help prevent hackers from accessing your system and prevent viruses and other malware from running in your system.

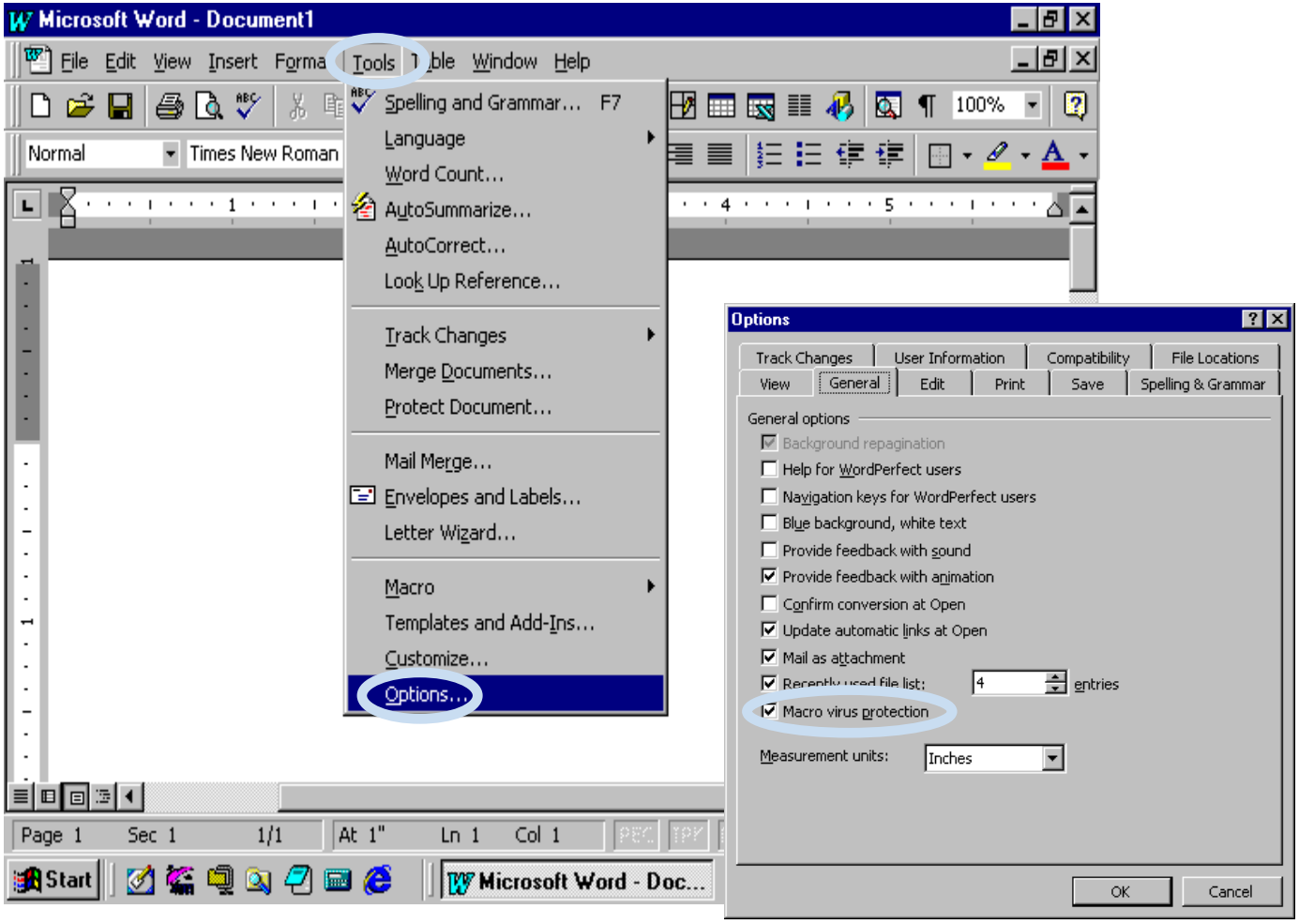
In order to close off security holes that have been discovered since Windows was shipped and installed, it is advisable that users visit the Microsoft Update Web site at http://windowsupdate.microsoft.com. The Web site has instructions provided that are easy enough to follow in updating your system.



Safe Computing Tips & Techniques

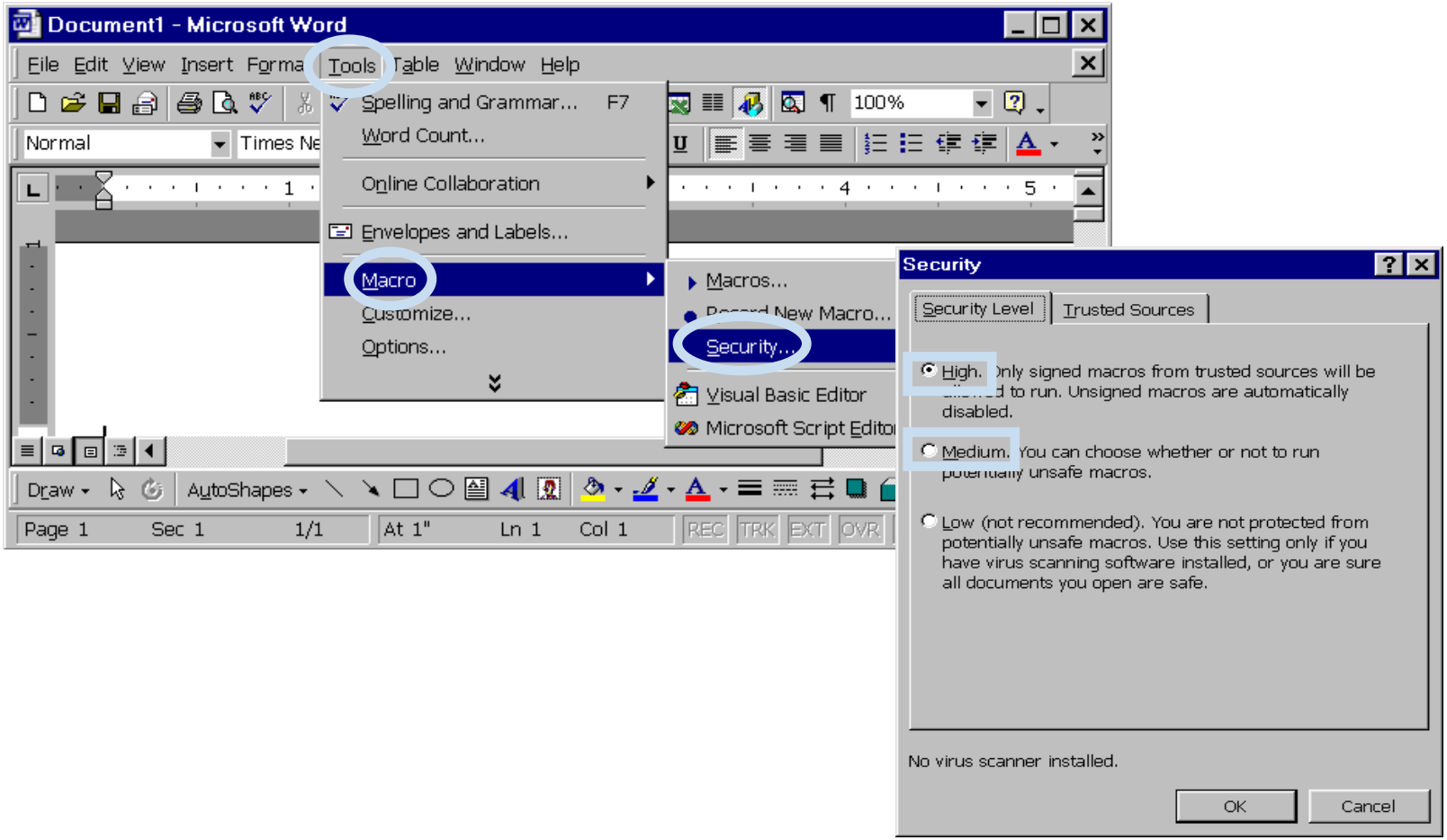
Enabling Macro Virus Protection

For MS Office 95 and MS Office 97



Safe Computing Tips & Techniques

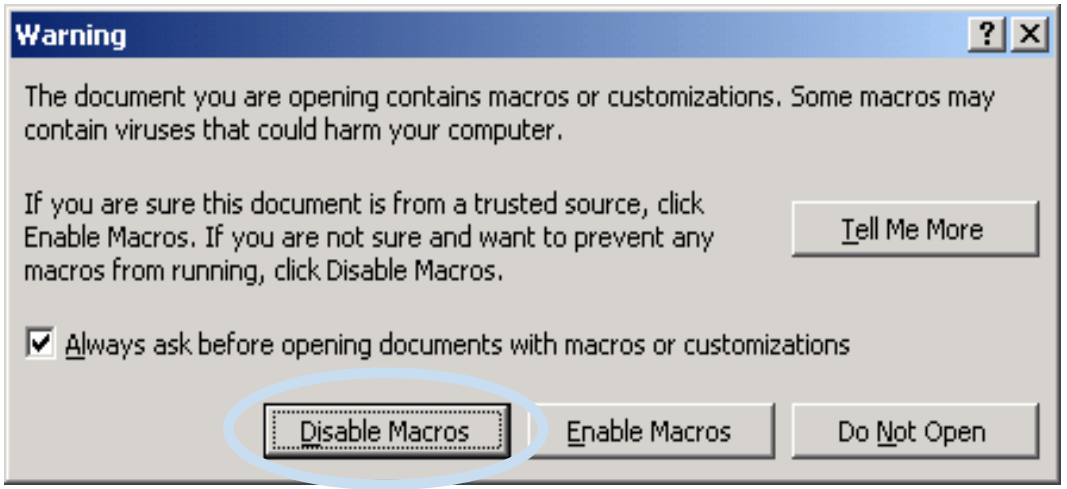
Enabling Macro Virus Protection For MS Office 2000



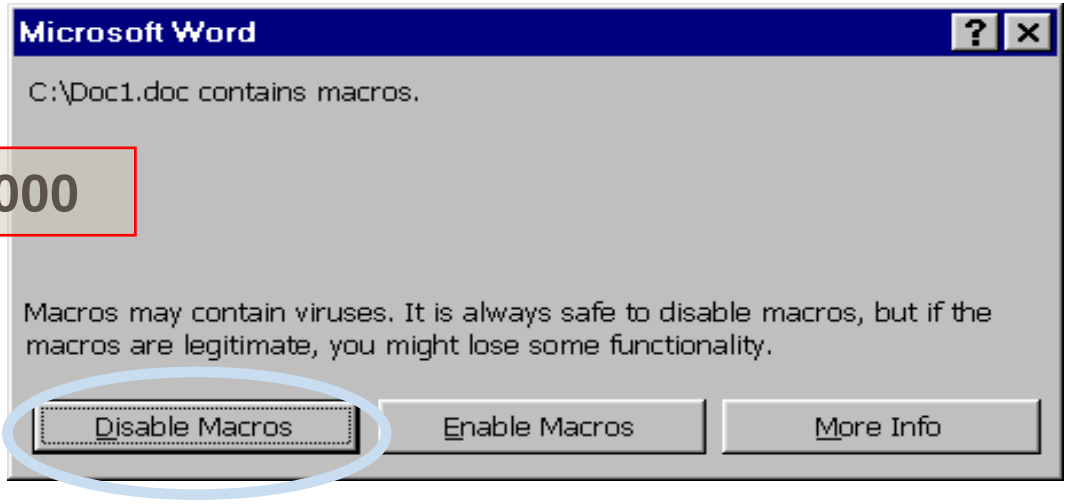
Safe Computing Tips & Techniques

Disabling Macros when prompted

For MS Office 95 and 97

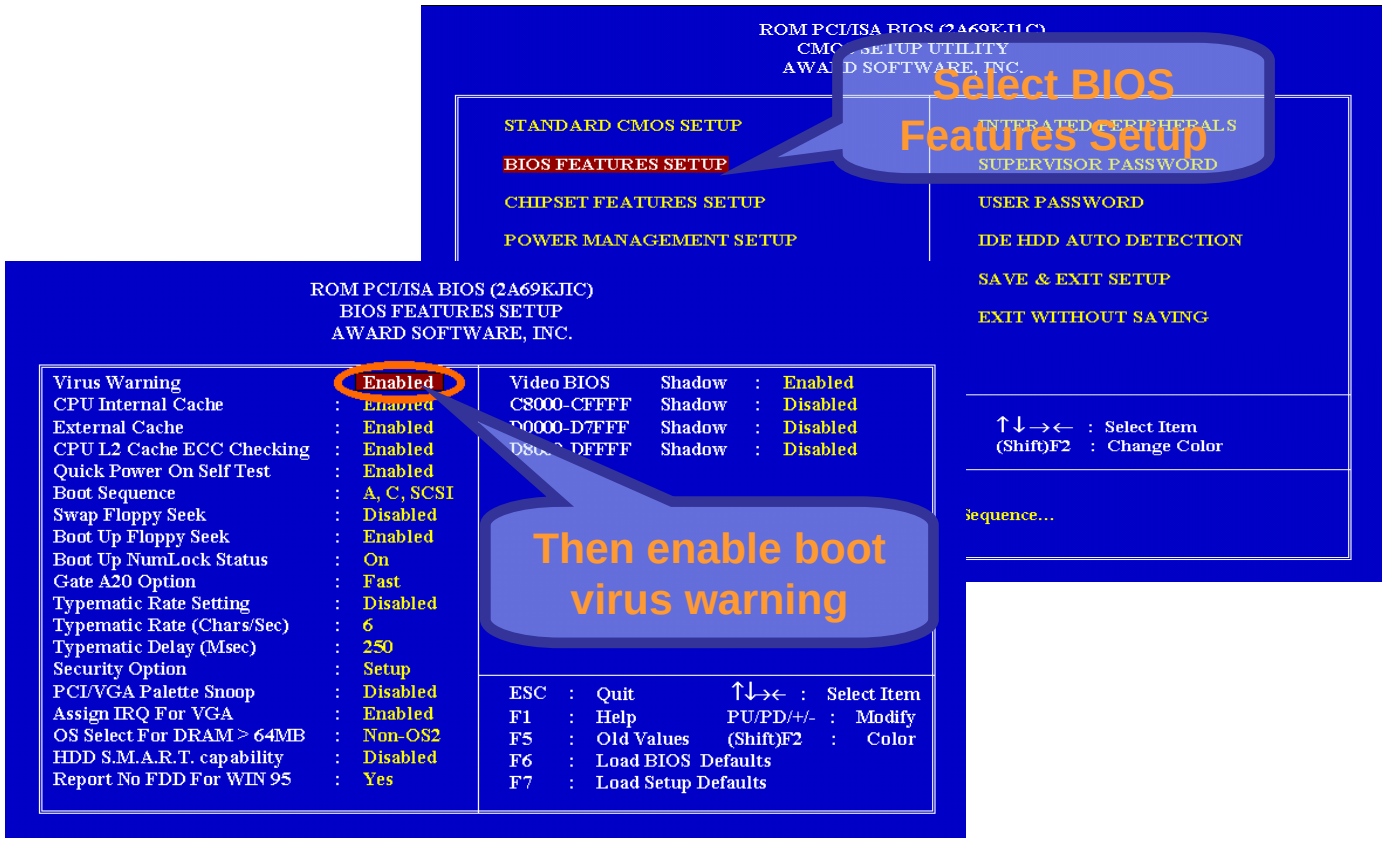


For MS Office 2000



Safe Computing Tips & Techniques

- Scan floppy diskettes before use
- Enable Virus Warning in CMOS setup



Safe Computing Tips & Techniques

Safe computing practices

- make it more difficult for malicious codes to enter or execute on client systems.
- add a protective layer of defense to prevent viruses and other malware from running.
- should always be followed in conjunction with updating antivirus software.