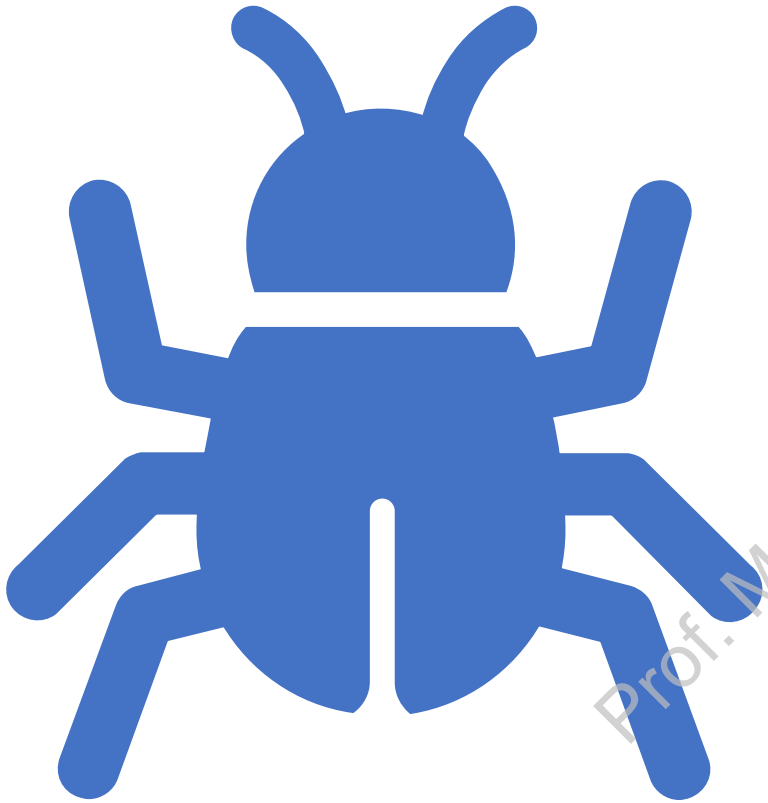


Non-malicious Program Errors vs Malicious Codes - Virus

By

Prof. Muhammad Iqbal Bhat

Government Degree College Beerwah

Topics

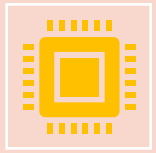
Non-malicious Program Errors

Malicious Codes - Virus

Non-malicious Program Errors:

Non-malicious program errors refer to a broad category of errors that can occur in software programs.

These errors are unintentional and result from mistakes made during the design, coding, or testing phases of software development.



Non-malicious program errors can cause a wide range of issues, from minor glitches to catastrophic failures that can compromise the security of the system or the data it contains.

Types of Non-malicious Program Errors:

Syntax Errors: These occur when the programmer violates the rules of the programming language. Syntax errors are usually detected by the compiler, which reports the error and prevents the program from running.

Runtime Errors: These occur when a program is running and encounters an unexpected situation that it cannot handle. Runtime errors can be caused by a wide range of issues, including input errors, hardware failures, and memory leaks.

Logic Errors: These occur when a program produces incorrect output due to a flaw in the design or coding of the program. Logic errors can be difficult to detect and correct, as they do not cause the program to crash or report an error.

Resource Errors: These occur when a program fails to manage system resources, such as memory or file handles, properly. Resource errors can cause a program to crash or behave unpredictably.

Impact of Non-malicious Program Errors:

- Non-malicious program errors can have a significant impact on the security of a system.
- In some cases, these errors can be exploited by attackers to gain unauthorized access to the system or to extract sensitive information.
- For example, a logic error in a web application could allow an attacker to bypass authentication controls and access sensitive data.

Preventing Non-malicious Program Errors:

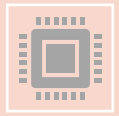
- The best way to prevent non-malicious program errors is to follow good software development practices.
- This includes using well-established programming languages, writing clear and concise code, and testing the software thoroughly before deployment.
- Code reviews and automated testing can also help to identify and correct errors before they become a problem.

Malicious Codes – Virus:

- Malicious codes are programs designed to cause harm to a system or its users.
- Viruses are one type of malicious code that can replicate themselves and spread from one system to another.
- Viruses are typically attached to legitimate files or programs and can infect a system when the user opens or runs the infected file.
- Once a virus infects a system, it can perform a wide range of malicious activities, including deleting files, stealing sensitive information, and using the infected system to launch attacks against other systems.

Types of Viruses:

File infectors: These viruses infect executable files, such as .exe or .com files. When the infected file is run, the virus is activated and can spread to other files on the system.



Boot sector viruses: These viruses infect the boot sector of a disk, making it difficult to remove the virus without reformatting the entire disk.

Macro viruses: These viruses infect macro-enabled documents, such as Microsoft Word or Excel files. When the infected document is opened, the virus is activated and can spread to other documents on the system.

Polymorphic viruses: These viruses are designed to evade detection by changing their code each time they replicate. This makes it difficult for antivirus software to detect and remove the virus.

Effects of Virus Infections:

- Slowing down of the system
- Frequent crashes and freezes
- Unauthorized access to personal or sensitive information
- Theft of identity and financial data
- Loss of critical data and files
- Disruption of normal business operations

Preventing Virus Infections:

- Avoid downloading and opening email attachments or files from untrusted sources.
- Keep the operating system and all software applications up to date with the latest security patches and updates.
- Use strong and unique passwords for all accounts and change them regularly.
- Use a firewall to block unauthorized access to the system.
- Backup critical data and files regularly and keep the backup copies in a safe place.

Conclusion:

Virus infections can cause serious harm to a system and its users. Understanding the different types of viruses and taking preventive measures can help to protect the system from virus infections. Antivirus software and other security measures should be regularly updated to stay ahead of the evolving threats posed by viruses and other malicious codes.