# IT 6823 LM 7. Malware

# Learning Material

**Note**: The learning material is composed of a list of web links, videos, and other materials screened and/or created by the instructor. The material is organized by student outcomes. Essential information is included in this document and students are recommended to go to the links to learn more about a specific topic.

## Overview

The module gives an overview of different types of malware, actors involved in malware attacks and how to protect against malware attacks.

Protect against malware is a part of Protect phase in the NITS security framework.

## Student Learning Outcomes

* **Describe major types of malware.**
* definition – “an umbrella term that describes any malicious program or code that is harmful to systems.
* Major types of malware – “What are the most common forms of malware”? section of the source below. Need to recognize the major types of malware.
* Source: <https://www.malwarebytes.com/malware/>
* 

Image source: <https://en.wikipedia.org/wiki/Malware#Security_defects_in_software>

* **Explain the characters of computer virus and ransomware**
* A computer virus works in much the same way as human flu:
	+ A computer virus requires a host program.
	+ A computer virus requires user action to transmit from one system to another.
	+ A computer virus attaches bits of its own malicious code to other files or replaces files outright with copies of itself.
* Virus vs. Trojan, worm, ransomware, rookit, and software bug. –“Computer virus examples” section of the source below.

Source: <https://www.malwarebytes.com/computer-virus/>

* Ransomware -definition and major types- source: <https://www.malwarebytes.com/ransomware/>
* **Describe how social engineering work**

Focus on the human vulnerabilities of social engineering and different type of social engineering.

Source: <https://www.malwarebytes.com/social-engineering/>

* **Discuss different types of inside threats and hacker**
	+ Insider threats. Source: <https://www.imperva.com/learn/application-security/insider-threats/>
	+ Hacker. Source: <https://www.malwarebytes.com/hacker/>
* **Explain the role of Firewall in protecting the computer system**

Source: <https://us-cert.cisa.gov/ncas/tips/ST04-004>

* **Discuss the best practices against malware attacks & inside threats**
* Factors make a system more vulnerable to malware.
	+ Security defects in software
	+ Insecure design or user error
	+ Over-privileged users and code
	+ Use of the same operating system

“Vulnerability” section of the source: <https://en.wikipedia.org/wiki/Malware#Security_defects_in_software>

* Malware attacks
	+ Continuous User Education
	+ Use Reputable A/V Software
	+ Ensure Your Network is Secure
	+ Perform Regular Website Security Audits
	+ Scanning your organization’s websites regularly for vulnerabilities
	+ Create Regular, Verified Backups

Source: <https://www.rapid7.com/fundamentals/malware-attacks/>

* Insider attack
	+ Protect critical assets
	+ Enforce policies
	+ Increase visibility
	+ Promote culture changes

Best practice and Insider Threat Detection Solutions of theSource: <https://www.imperva.com/learn/application-security/insider-threats/>