

**Name**: Eseigbe Joshua Oluwajoba

**ID**: 142017

**TOPIC**: Computer Security Threats and Techniques

**Table of Contents**

[1. Introduction 3](#_Toc62839741)

[1.1. Definition Of Compuer Security 3](#_Toc62839742)

[1.2. Definition Of Compuer Threats 3](#_Toc62839744)

[2.0. Types Of Computer Threats 3](#_Toc62839745)

[2.1. Computer Virus 3](#_Toc62839746)

[2.1.1. Cryptolocker 4](#_Toc62839747)

[2.1.2. Mydoom 4](#_Toc62839750)

[2.1.3. Stuxnet 4](#_Toc62839751)

[2.2. Trojan Horses 4](#_Toc62839752)

[2.3 Spyware 4](#_Toc62839753)

[2.4. Worms 5](#_Toc62839754)

[2.5. Phishing 5](#_Toc62839755)

[2.6. Ransomware 6](#_Toc62839756)

[2.7. Hacking 6](#_Toc62839757)

[2.8. Natural Disasters 6](#_Toc62839758)

[3.0. Stages Of Computer Attacks 6](#_Toc62839759)

[4.0 Computer Protection Counter Measures 7](#_Toc62839760)

[4.1 Software Security Measures 8](#_Toc62839761)

[4.1.1 Firewalls 8](#_Toc62839762)

[4.1.2 Cryptography 8](#_Toc62839764)

[4.1.3. Antivirus Software: 8](#_Toc62839765)

[4.1.4. Anti-Spyware Package 8](#_Toc62839766)

[4.2. Hardware Security Measures 8](#_Toc62839767)

[4.2.1. Computer Case Intrusion Detection 8](#_Toc62839768)

[4.2.2. Trusted Platform Modules 9](#_Toc62839769)

[5.0. Conclusion 9](#_Toc62839770)

[5.0.1. Importance Of Computer Security 9](#_Toc62839771)

[6.0. Bibliography 10](#_Toc62839772)

# **INTRODUCTION**

Computer threats come in all forms, software or hardware-based threats. It could be as simple as buggy applications causing glitch in software systems, to invasive viral hacks that could potentially make the best computer hardware irreparable.

Hence the need for a thorough understanding on the various ways in which a computer system can be at risk to threats.

# **DEFINITION OF COMPUER SECURITY**

# Computer security is the protection of [computer systems](https://en.wikipedia.org/wiki/Computer_system) and [networks](https://en.wikipedia.org/wiki/Computer_network) from the theft of or damage to their [hardware](https://en.wikipedia.org/wiki/Computer_hardware), [software](https://en.wikipedia.org/wiki/Software), or [electronic data](https://en.wikipedia.org/wiki/Data_(computing)), as well as from the [disruption](https://en.wikipedia.org/wiki/Denial-of-service_attack) or [misdirection](https://en.wikipedia.org/wiki/Botnet) of the services they provide.Another name for this term include cybersecurity.

# **DEFINITION OF COMPUER THREATS**

In [computer security](https://en.wikipedia.org/wiki/Computer_security), a threat is a potential negative action or event facilitated by a [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) that results in an unwanted impact to a computer system or application.

Herein, the term “threat”  is defined as any kind of software potentially or directly capable of inflicting damage to a computer or network and compromising the user's information or rights (that is, malicious and other unwanted software). In a wider sense, the term "threat" may be used to indicate any type of potential danger to the security of the computer or network (that is, vulnerabilities that can result in hacker attacks).

# **2.0. TYPES OF COMPUTER THREATS**

# **2.1. COMPUTER VIRUS**

A computer virusis a type of [computer program](https://en.wikipedia.org/wiki/Computer_program) that, when executed, replicates itself by modifying other computer programs and [inserting](https://en.wikipedia.org/wiki/Code_injection) its own [code](https://en.wikipedia.org/wiki/Computer_language). If this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Viruses usually require a host program. A host program is a program in which the virus writes its own code into.

Below are examples of computer virus:

# **2.1.1. CryptoLocker**

# Released in September 2013, CryptoLocker spread through email attachments and encrypted the user’s files so that they couldn’t access them.

# The hackers then [sent a decryption key in return for a sum of money](https://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/), usually somewhere from a few hundred pounds up to a couple of grand.

# **2.1.2. MyDoom**

MyDoom, like ILOVEYOU, is a record-holder and was the fastest-spreading email-based worm ever. MyDoom was an odd one, as [it hit tech companies like SCO, Microsoft, and Google with a Distributed Denial of Service](https://en.wikipedia.org/wiki/Mydoom) attack.

# **2.1.3. Stuxnet**

Stuxnet spread by a USB thumb drive and targeted software controlling a facility in Iran that held uranium. [The virus was so effective it caused their centrifuges to self-destruct](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=2&_r=3&seid=auto&smid=tw-nytimespolitics&pagewanted=all&), setting Iran’s nuclear development back and costing a *lot* of money.

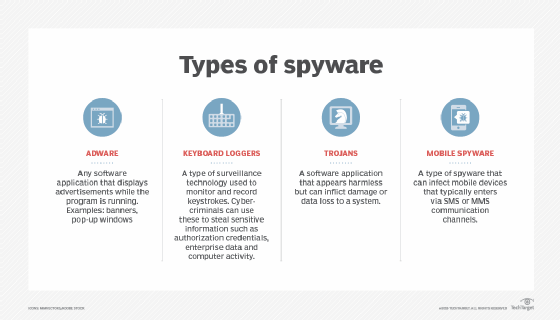
Stuxnet is the first real venture into cyberwar and it definitely asks the question as to what will come next. The idea of digital weaponry is pretty scary, isn’t it?

# **2.2. TROJAN HORSES**

Trojan horse is a [malicious code](https://cyberthreatportal.com/malware-definition-and-example/) or program that developed by hackers to disguise as legitimate software to gain access to organization’s systems. It has designed to delete, modify, damage, block, or some other harmful action on your [data](https://en.wikipedia.org/wiki/Data) or [network](https://en.wikipedia.org/wiki/Computer_network).The victim receives an email with an attachment file which is looking as an original official email. The attachment file can contain malicious code that is executed as soon as when the victim clicks on the attachment file.

# **2.3 SPYWARE**

Spyware is unwanted **types of security threats to organizations** which installed in user’s computer and collects sensitive information such as personal or organization’s business information, login credentials and credit card details without user knowledge.This type of threats monitor your internet activity, tracking your login credentials, and spying on your sensitive information.



*Figure 1: Types of Spyware*

# **2.4. WORMS**

Computer worm is a type of [malicious software](https://enterprise.comodo.com/blog/what-is-malicious-software/) or program that spreads within its connected network and copies itself from one computer to another computer of an organization.It can spread without any human assistance and exploit the security holes of the software and trying to access in order to stealing sensitive information, corrupting files and installing a back door for remote access to the system.

# **2.5. PHISHING**

Phishing is a type of[social engineering](https://en.wikipedia.org/wiki/Social_engineering_(security)) attack that attempt to gain confidential information such as usernames, passwords, credit card information, login credentials, and so more.

* In a phishing email attack, an attacker sends phishing emails to victim’s email that looks like it came from your bank and they are asked to provide your personal information.
* The message contains a link, which redirects you to another [vulnerable](https://en.wikipedia.org/wiki/Vulnerability) website to steal your information.
* So, it is better to avoid or don’t click or don’t open such type of email and don’t provide your sensitive information.

# **2.6. RANSOMWARE**

Ransomware is type of security threats that blocks to access computer system and demands for bitcoin in order to access the system. The most dangerous ransomware attacks are  [WannaCry](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack), Petya, Cerber, Locky and [CryptoLocker](https://en.wikipedia.org/wiki/CryptoLocker) etc. This is an example of a computer threat that can render the hardware of a computer system useless.

# **2.7. HACKING**

This is defines as gaining unauthorized access to a computer system or private network. People who engage in this activity are called hackers. This may be through the use of brute force techniques with physical contact to the computer systems or it could be remote controlling of the processes and services of a computer system.

# **2.8. NATURAL DISASTERS**

Fire, flood, etc. can cause loss of computers and data. Either fire or water can cause a hard disk drive failure, for example. Earthquakes can cause a data center to go down. For this reason large web businesses use [load balancing](https://en.wikipedia.org/wiki/Load_balancing_(computing)) and [failover](https://en.wikipedia.org/wiki/Failover) techniques to ensure [business continuity](https://en.wikipedia.org/wiki/Business_continuity).

# **3.0. STAGES OF COMPUTER ATTACKS**

**Step 1: Spoofing**

Before initiating any of the attacking steps, the hackers normally prefer to hide their identity and their activities. These are normally done by spoofing when the attacker hides his identity and pretends to be someone else. This can be done by MAC cloning, IP spoofing, or email spoofing.

**Step 2: Reconnaissance**

It is always a good practice to plan well before undertaking any action, and this is applicable in the case of hacking too. The hackers first identify a target to launch an attack, extract maximum information regarding this target, understand its vulnerabilities, and then only explore the best ways to exploit it.

Step 3: Weaponization

The hacker with the information collected in the previous phase identifies/develops weapons in order to get into the computer or the network. During this phase, the hacker collects the tools that they plan to use once they gain access to the system for the successful exploitation of the vulnerabilities in the system.

**Step 4: Implementation**

In the implementation phase, the attack starts working. It is when the phishing e-mails are sent or when the fake web pages are posted to the Internet and the attacker patiently waits for all the data, they need to start rolling in.

**Step 5: Exploitation**

This is a state when the sensitive and confidential data starts rolling in. It is the most exciting phase for the hackers, and they try out the usernames and passwords against web-based e-mail systems or secured connections to sensitive networks.

**Step 6: Installation**

After a successful exploitation, the attacker will make sure to have continued access to the system. This is by installing a persistent backdoor or creating admin accounts on the system, disabling firewall rules, and perhaps even activating remote desktop access on computer systems on the network.

**Step 7: Control**

Once the attacker gains access to the network or creates administrator accounts or installs all the necessary tools for backdoor entry any time to the system, the attacker is in control of the target.

**Step 8: Action on set goals**

With total control on the target system, the attacker can set goals and achieve it with or without the knowledge of the genuine user.

The attacks are thus classified depending on the various steps taken by the hacker in the process of the attack, starting from hiding the identity to information collection, which is the pre-phase of an attack, to the actual attack.

# **4.0 COMPUTER PROTECTION COUNTER MEASURES**

A counter measure is a procedure that minimizes the risk of vulnerability or attack on a system by directly stopping the harm it causes or by reporting to ensure corrective precautions.

# **SOFTWARE SECURITY MEASURES**

# **FIREWALLS**

# [Firewalls](https://en.wikipedia.org/wiki/Firewall_(networking)" \o "Firewall (networking)) are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be both hardware- or software-based.

# **4.1.2 CRYPTOGRAPHY**

Cryptography is he method of securing data and communications through the use of codes, cyphers and encryption techniques.

# **4.1.3. ANTIVIRUS SOFTWARE:**

Antivirus is a kind of software used to prevent, scan, detect and delete viruses from a computer. [Antivirus software](https://www.business.com/categories/best-antivirus-and-internet-security/) plays a major role in protecting your system by detecting real-time threats to ensure your data is safe. Some advanced antivirus programs provide automatic updates, further protecting your machine from the new viruses that emerge every day. After you install an antivirus program, don't forget to use it. Run or schedule regular virus scans to keep your computer virus-free.

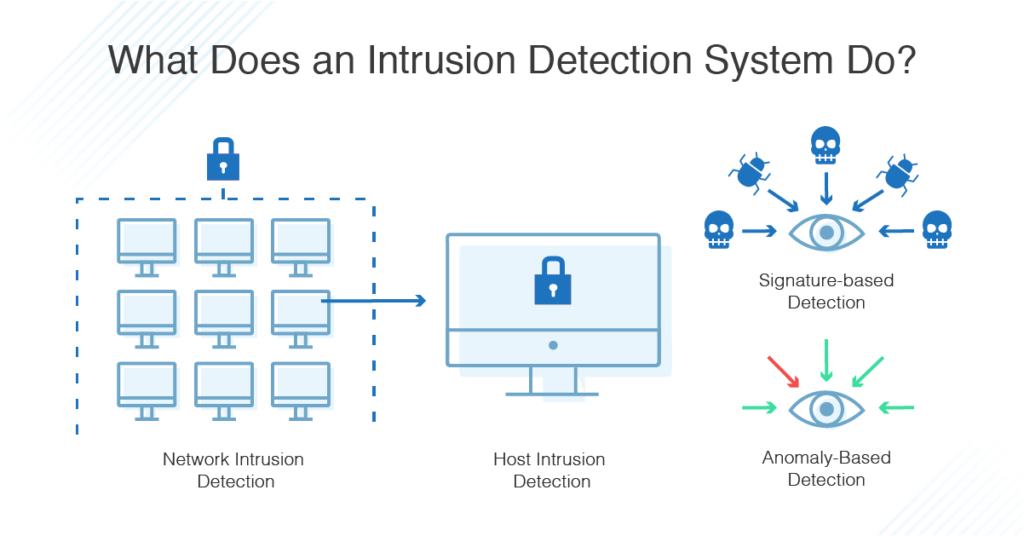
# **4.1.4. ANTI-SPYWARE PACKAGE**

Some spyware records every keystroke to gain access to passwords and other financial information. Anti-spyware concentrates exclusively on this threat, but it is often included in major antivirus packages, like those from [Webroot](https://www.webroot.com/us/en). Anti-spyware packages provide real-time protection by scanning all incoming information and blocking threats.

# **4.2. HARDWARE SECURITY MEASURES**

# **4.2.1. COMPUTER CASE INTRUSION DETECTION**

Refers to a device, typically a push-button switch, which detects when a computer case is opened. The firmware or BIOS is programmed to show an alert to the operator when the computer is booted up the next time.



*Figure 2: Intrusion Detection System*

# **4.2.2. TRUSTED PLATFORM MODULES**

(TPMs) secure devices by integrating cryptographic capabilities onto access devices, through the use of microprocessors, or so-called computers-on-a-chip. TPMs used in conjunction with server-side software offer a way to detect and authenticate hardware devices, preventing unauthorized network and data access.

# **5.0. CONCLUSION**

# **5.0.1. IMPORTANCE OF COMPUTER SECURITY**

The main purpose of the security is the preventing and detecting unauthorized access of computer system. It guarantees to safe processing and storage of business, healthcare and sensitive information.

1. To protect personal information
2. Prevention of data theft
3. Prevention of viruses and malware
4. To protect organization assets

Threats to computer systems have existed since the first computers and while it is impossible to mark every possible source of danger, it is important to be precautious and always take preventive measures to avoid compromise of computer systems. Although many threats to the computers have solutions today, it is very necessary to avoid in all forms because they can cause permanent loss of data as well as permanent damage to hardware components. Hence the need to have a good knowledge of computer security systems.

# **6.0. BIBLIOGRAPHY**

1. Computer security: <https://en.wikipedia.org/wiki/Computer_security>

# The 8 Most Famous Computer Viruses of All Time: <https://uk.norton.com/norton-blog/2016/02/the_8_most_famousco.html>

1. Computer Virus: <https://en.wikipedia.org/wiki/Computer_virus>
2. Common types of security threat to organizations: https://cyberthreatportal.com/types-of-security-threats-to-organizations/
3. Threats: <https://en.wikipedia.org/wiki/Threat_(computer)>
4. Computer security threats:

https://www.intechopen.com/books/computer-security-threats/introductory-chapter-computer-security-threats

1. 18 ways to protect your devices from hackers: <https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html>
2. Antivirus: <https://www.verizon.com/info/definitions/antivirus/>
3. Outline of computer security: <https://en.wikipedia.org/wiki/Outline_of_computer_security#:~:text=Computer%20security%20includes%20measures%20taken,accessing%20the%20data%2C%20and%20providing>
4. Top reasons why computer security is important:

https://cyberthreatportal.com/why-is-computer-security-important/