**CYBERYOUTH**

**Nonformal education for cyber-security training & resilience of youth organisations and young people**

***Cybersecurity online youth academy***

****

**Core Cybersecurity Principles**

Table of contents

[Introduction](#_heading=h.fpb3yt6tcffi)

[It could have happened to you…](#_heading=h.c7zxm1r80lor)

[What you will learn](#_heading=h.bd1t10x6k115)

[Why it is important](#_heading=h.1fqj6c1n3ygs)

[How it can help you in everyday life](#_heading=h.bddh90wxykhs)

[What career you can pursue](#_heading=h.l25siuf1d90q)

[Pre-requisites](#_heading=h.obikvf4haym5)

[Material](#_heading=h.snpqznqbwxs)

[1.1 What is Information Security](#_heading=h.2yz7x8bu8zb5)

[Definition](#_heading=h.rodcxh44by7b)

[The CYBERYOUTH online training course](#_heading=h.5yvus9wl5g1)

[1. Core Cybersecurity Principles](#_heading=h.sb35t8oh2ty1)

[Conclusions](#_heading=h.q7y4utybp22l)

[1.2 CIA Triad](#_heading=h.wv8lmqsplpdd)

[What is the CIA standard:](#_heading=h.3ggz09tbdpv3)

[Confidentiality](#_heading=h.qdq5bedkcsun)

[Integrity](#_heading=h.gao5qw8o0cvy)

[Availability](#_heading=h.ygm45ri87jbx)

[Best practices and brief history of the CIA triad](#_heading=h.ue6y3nap4th4)

[Conclusions](#_heading=h.jn7khpgf6mc9)

[1.3 Hacker Culture](#_heading=h.g98km9urykdd)

[The term “hacker”](#_heading=h.w3h9p5vfecpt)

[Conclusions](#_heading=h.ostdn54761l3)

[1.4 Operating Systems](#_heading=h.7pii0khen2cd)

[Windows](#_heading=h.92ae3r8jez9v)

[Conclusions](#_heading=h.8fgh3pvuc4s3)

[1.5 Networking](#_heading=h.5getcl4kti7b)

[Definition](#_heading=h.3d9i8b28vnbj)

[Key components](#_heading=h.2rk0lh3zuhwj)

[Internet protocol suite](#_heading=h.dhc96m3l441)

[OSI model (the 7 layers)](#_heading=h.evqwix3bx5y5)

[Conclusions](#_heading=h.scbfee5behhv)

[1.6 System Administration](#_heading=h.hxk9abfklxgp)

[Gnu/Linux](#_heading=h.iocb49ut3yab)

[Windows](#_heading=h.pgrlyzs0r8a2)

[Conclusions](#_heading=h.nmzwup8r2vh3)

[1.7 The Jargon File](#_heading=h.syt91kbcyrsy)

[The Geek’s Corner](#_heading=h.floxyjcfjlz3)

[Conclusions](#_heading=h.umqq3lf4f2yk)

[Quiz](#_heading=h.35btfg6prjdy)

[References](#_heading=h.ioedg3ublhq7)

# 

# **Introduction**

## **It could have happened to you…**

A seemingly routine day could take an unexpected turn. In a busy workplace setting a conscientious youth worker accidentally clicked on a dubious email attachment while focused on the next Erasmus adventure. She was unaware that it released a malicious payload that had stealthily entered the entire office network. The breach started to take shape gradually but surely. System files were encrypted, making it impossible to access vital information. When coworkers realised their accounts had been stolen and private information was in the wrong hands, panic broke out. Some youth workers who had IT training before responded quickly to the breach, containing the situation, restoring the system from backups, and quickly putting in place tighter security measures. Such an incident could serve as a sobering reminder that cyber risks could exist in even the mundane office environment or workplace. Such events highlight the significance of vigilance, employee understanding and strong cybersecurity measures.

## **What you will learn**

In this Unit you will learn about the core principles of cybersecurity. We answer the questions “What is Information Security?”, “What are the core cybersecurity principles, “What is the CIA standard?”. We will look at the best practices and brief history of the CIA triad as well as an overview of the hacker culture. Some of the operating systems will be explored as well as some important aspects of networking and system administration. At the end of the Unit you could spend some extra time exploring “The Geek’s corner” which will contain more detailed and in-depth information about the issues covered. Finally you could self-assess your new knowledge with the interactive Quiz.

## **Why it is important**

Due to the ubiquitous and constantly changing nature of cyber threats in today's interconnected digital environment, cybersecurity has become more and more important. The need for effective cybersecurity measures to reduce risks, foster trust, and protect the fundamentals of a safe digital ecosystem develops along with our reliance on technology.

Furthermore the CyberYouth field research has pointed to the urgent need of cybersecurity training for youth organisations and youth workers. Young people involved in the field research have also pointed out that they recognize cybersecurity as important and would like to learn more about how to protect themselves in daily life.

## **How it can help you in everyday life**

In this Unit you will be introduced to the core principles of cybersecurity. This information will help you to be more aware of the common jargon and concepts related to information security. It will also improve your potential to recognize cyber threats in daily life and protect your information and your security better. The Unit also covers some history and issues related to different spheres of work such as system administration, networking etc. which could help with the awareness of different job opportunities in this field.

## **What career you can pursue**

Some possible careers related to the topics covered in this Unit:

* Information Security Analyst
* Penetration Tester (Ethical Hacker)
* Security Engineer
* Cyber Security consultant
* Incident Response Analyst
* Security Architect
* Forensic Analyst
* System administrator

## **Pre-requisites**

To study this module the learner needs to have at least a basic understanding of ICT and how to work with computers and the Internet. Additionally interest in the topic and enthusiasm to learn and explore new skills is a plus.

# 

# 

# 

# **Material**

## **1.1 What is Information Security**

## **Definition**

Information security, or **InfoSec**, is the term used to describe the procedures and devices created and used to safeguard confidential data against change, interruption, destruction, and inspection. InfoSec strives to protect from internet dangers including hacking and data breaches as well as the confidentiality, availability, and integrity of data.

To stay ahead of changing hazards, organisations must continually evaluate and enhance their security measures. To protect sensitive data and systems, a combination of technical solutions, policy, and employee involvement is required.

**What distinguishes information security from cybersecurity?**

**Cybersecurity** and information security are frequently mixed up. Although it only refers to the procedures created for data security, infosec is an essential component of cybersecurity. Information security (InfoSec) is a more generic word for cybersecurity.

The importance of cybersecurity

There are numerous sorts of cybersecurity within the field of information security, as well as numerous procedures businesses can employ to safeguard their data and prevent a data breach. These include everything from the coding systems used to physically store hardware and plant materials properly to ensuring employees are properly trained and using protected devices to making sure your business has a proper incident response plan. It's crucial to cover all the bases, and enabling a robust and comprehensive cybersecurity plan can prove crucial for the success of any type of organisation as well as for the personal digital wellbeing of the individuals involved.

Due to the frequency and sophistication of cyber threats, cybersecurity is of utmost relevance for all types of enterprises. Organisations rely significantly on information systems and networks to store, process, and transport vital data in the current digital era. This information consists of private client information, proprietary information, financial information, and trade secrets. Organisations are vulnerable to cyberattacks without adequate cybersecurity safeguards in place, which can have serious repercussions like financial loss, reputational harm, legal obligations, and disruption of corporate activities.

The constantly changing nature of cyber threats is a major factor in why cybersecurity is so important. Cybercriminals are constantly coming up with new methods and plans to take advantage of weaknesses in networks and computer systems. They use a variety of strategies to obtain illegal access, steal data, or disrupt operations, including malware, phishing assaults, ransomware, and social engineering. Organisations may successfully detect, prevent, and respond to these threats by investing in strong cybersecurity solutions, thereby reducing the potential impact on their operations and safeguarding critical data.

Another important part of cybersecurity is adherence to legal and regulatory regulations. The **General Data Protection Regulation (GDPR)** in the **European Union and the Health Insurance Portability and Accountability Act (HIPAA)** in the healthcare industry are just two examples of the unique legislation that many businesses have in place to protect consumer data. Serious fines and legal repercussions may result from violating these restrictions. Employing robust cybersecurity measures guarantees that organisations follow these laws, uphold data privacy, and cultivate trust with their stakeholders and customers.

In conclusion, because of the complexity of cyberthreats and the necessity to adhere to legal and regulatory standards, cybersecurity is crucial for enterprises. Organisations may safeguard sensitive data, keep consumers' trust, reduce financial and reputational risks, and guarantee the efficient execution of their company processes by giving cybersecurity first priority.

Video: Cybersecurity: Crash Course Computer Science #31 <https://youtu.be/bPVaOlJ6ln0>

## The CYBERYOUTH online training course

By offering an open and flexible online training that covers the fundamentals, the CYBERYOUTH initiative seeks to provide non-formal education for cyber-security training & resilience of youth organisations and young people. The resources you are currently viewing were produced by youth organisations who regularly deal with young people as well as cybersecurity-focused organisations. The CYBERYOUTH online training course offers a distinctive and specialised approach to the subject with a special approach to young people and their needs by fusing cybersecurity experience, youth work, non-formal education methods and e-games.

The following topics are covered by the course:

## Core Cybersecurity Principles

1. Vulnerabilities, Attack, Techniques, and Threats
2. Secure System Architecture and Design
3. Implementation of Security solutions
4. Policies and Procedures for Incident Response
5. Governance, Risk and Compliance

The cyber-security app for youth empowerment through online gamified non-formal education is a gamified app that is useful for youth workers, youth & cybersecurity experts to

approach very practical everyday situations and reflect on them through games. It has been created with the cooperation of youth workers, young people and SMEs. You can learn more on <https://cyberyouthproject.com/>.

### **Conclusions**

In conclusion, because of the complexity of cyberthreats and the necessity to adhere to legal and regulatory standards, cybersecurity is crucial for all organisations especially those that work with young people. They may safeguard sensitive data, keep the trust of the people who’s information they work with, reduce financial and reputational risks, and guarantee the efficient execution of their company processes by giving cybersecurity a priority.

By combining cybersecurity expertise, youth work, non-formal education techniques, and e-games, the CYBERYOUTH training course offers a novel and specialised approach to the issue with a special approach to young people and their needs.

## 

## **1.2 CIA Triad**

## What is the CIA standard:

The Confidentiality, Integrity, and Availability (CIA) triad, which stands for the three fundamental tenets of information security, is a key idea in the field of cybersecurity. These guidelines provide a framework for creating and putting into place strong security measures that safeguard sensitive information and guarantee the efficient operation of networks and systems.

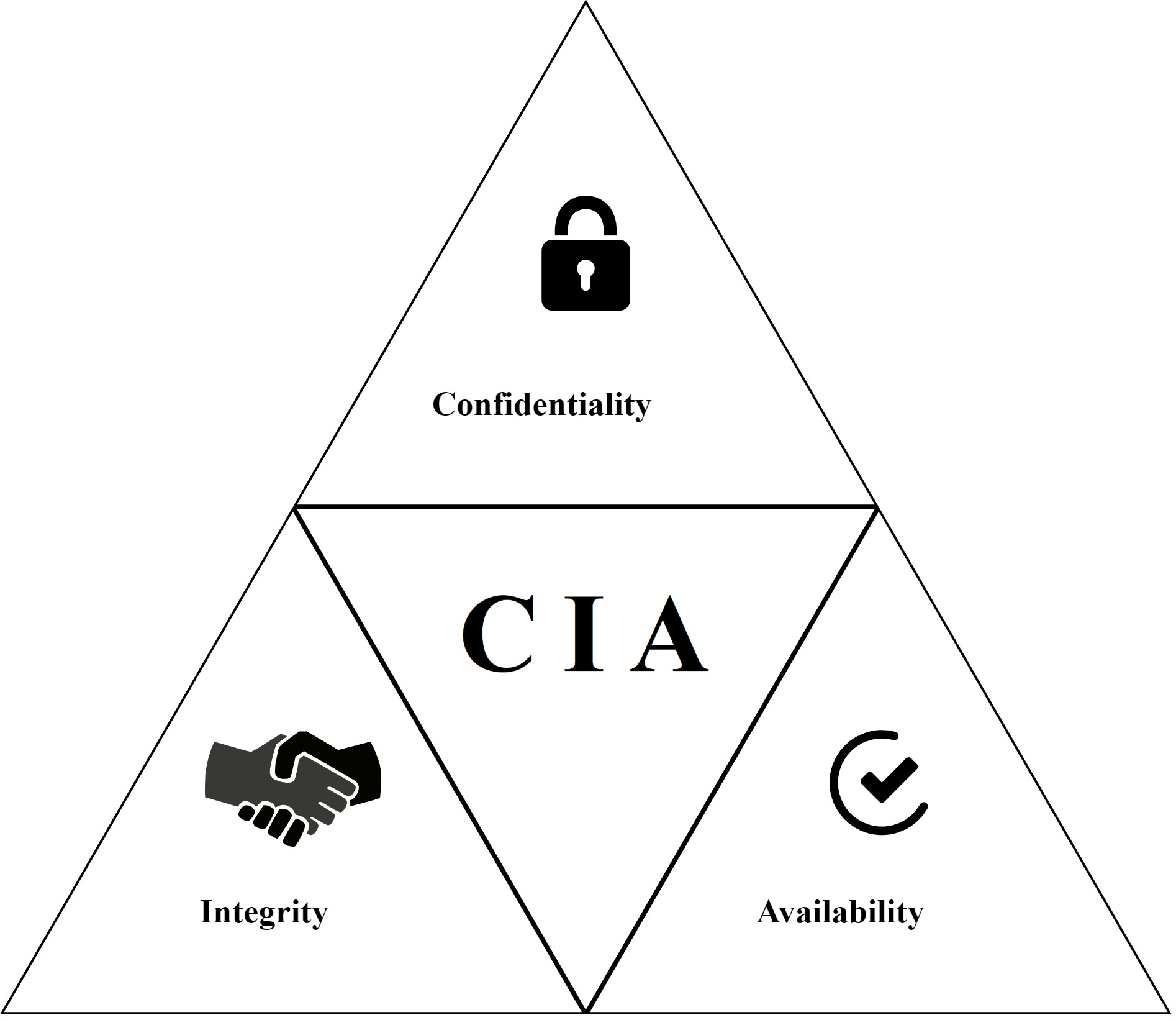


Image source: <https://openclipart.org/detail/339113/cia-triad>

## Confidentiality

Confidentiality is the first pillar of the CIA triad and refers to the protection of information from unauthorised access. It makes sure that only authorised people or organisations can access data. Strong authentication procedures, encryption mechanisms, and access controls are just a few examples of confidentiality measures. Organisations can protect sensitive information from unauthorised disclosure and inadvertent exposure by putting strong confidentiality safeguards in place.

## Integrity

The second CIA triangle principle, integrity, is concerned with preserving data's reliability and correctness during the course of its existence. It makes sure that data is protected and unmodified by unauthorised parties or malicious actions. Through techniques like data validation, checksums, digital signatures, and safe backup and recovery procedures, organisations may guarantee the integrity of their data. Organisations may be certain that their data has not been tampered with and can be relied upon for decision-making and business operations by ensuring data integrity.

## Availability

The third CIA tenet, availability, speaks to the usability and accessibility of data and resources when required. It entails making sure that data, networks, and systems are consistently accessible to authorised users. Through strategies like redundancy, fault tolerance, disaster recovery plans, and network monitoring, organisations can attain availability. Organisations can reduce downtime, guarantee continuous operations, and lessen the effects of unexpected interruptions or cyberattacks by prioritising availability.

It's critical to remember how closely related and dependent the three CIA triad concepts are. For instance, sustaining availability is aided by assuring confidentiality and integrity. The accessibility of information or systems may be jeopardised by unauthorised access or data tampering. Similarly, if a system goes down, it might make it harder to uphold integrity and secrecy. The CIA triad offers organisations a thorough framework for approaching information security, to sum up. Organisations can take the necessary security measures to safeguard sensitive data, preserve data correctness and reliability, and guarantee ongoing access to information and resources by taking the principles of confidentiality, integrity, and availability into consideration. For enterprises to manage risks efficiently, protect their assets, and keep stakeholders' trust and confidence, they must abide by the CIA triangle principles.

**Viedo**: What is the CIA Triad, IBM Technology, YouTube.com: <https://youtu.be/kPPFNrlN3zo>

## Best practices and brief history of the CIA triad

Here are some best practices for the implementation of the CIA triad:

* Employ a layered security approach: Organizations should employ numerous levels of security controls rather than relying exclusively on one security solution. This comprises security safeguards including firewalls, IDSs, encryption, access controls, and recurring security audits. A layered approach guarantees that other security measures are still in place to protect the organisation's assets even if one layer is compromised.
* Identify potential hazards to your organisation's information assets by conducting frequent risk assessments. This includes assessing security gaps, prospective threats, and the effects of a security breach. Organisations may efficiently prioritise security initiatives and manage resources by being aware of their threats.
* Maintaining employee awareness and training is important since security breaches frequently result from human mistakes. In order to inform employees on cybersecurity best practices, the value of data protection, and the potential hazards associated with their actions, organisations should invest in frequent training programs. An organisation's overall security posture can be greatly improved by fostering a culture of security awareness among its workforce.
* Update and patch systems frequently: Vendors regularly offer updates and patches to address newly found software and hardware vulnerabilities. Organisations should have a clear procedure in place for updating and patching their systems on a regular basis to keep them safe from the most recent threats.
* Backup and disaster recovery planning: To sustain availability and recover from potential incidents, regular backups of vital data and the implementation of strong disaster recovery plans are essential. Establishing a dependable backup strategy, performing routine backups, and occasionally testing disaster recovery plans are all things that organisations should do to ensure their effectiveness.

Brief history overview of the CIA Triad:

The CIA Triad was first introduced in the early days of information security, and it has since developed to keep up with the evolving threat environment. The U.S. Department of Defense created a security model known as the Bell-LaPadula model in the 1960s, which is when the CIA trinity first emerged. The values of integrity and confidentiality were emphasised in this model.

The National Bureau of Standards, which is now known as the National Institute of Standards and Technology (NIST), added the availability notion to the security model in the 1970s. The CIA Triad was completed with this contribution.

The CIA Triad has since evolved into a mainstay of information security procedures and systems. It serves as the foundation for creating security controls and putting in place security measures, and it has been widely embraced across numerous industries. The ISO 27001 and NIST Cybersecurity Framework, which offer rules for enterprises to maintain and improve their cybersecurity posture, were both developed with input from the CIA Triad.

### **Conclusions**

The CIA triad has evolved with changing technology and dangers while continuing to be relevant over time. The CIA Triad continues to be a vital foundation for enterprises to protect their data, maintain its integrity, and assure its availability in light of the complexity of cyber threats and the expanding value of digital information.

## **1.3 Hacker Culture**

## The term “hacker”

Initially, the term "hacker" was used to describe those who were very skilled and knowledgeable in computer programming and system security. However, the way people view hackers has changed over time, and now there are two separate subcultures of hackers: ethical hackers and malicious hackers.

****

Computer hacker, Image source: <https://openclipart.org/detail/308848/computer-programer>

Types of Hackers

Ethical Hacker Culture: **White hat** hackers, commonly referred to as ethical hackers, are those who utilise their technical knowledge to find and close security holes in networks and computer systems. They are frequently used by businesses to carry out security audits, penetration tests, and vulnerability analyses since they operate within moral and legal bounds. A code of behaviour that places an emphasis on responsible disclosure and the defence of user privacy and data is followed by ethical hackers. They are motivated by a desire to increase system security and a curiosity about how systems function.

Malicious Hacker Culture: Malicious hackers engage in damaging and illegal acts. They are also known as **black hat** hackers or cybercriminals. They take advantage of holes in computer programs and networks to commit crimes against themselves such as money fraud, data theft, and service interruption. Malicious hackers are driven by monetary rewards, political objectives, or personal grudges. Their acts are illegal and frequently have detrimental effects on people and organisations.

**Video:** Hackers & Cyber Attacks: Crash Course Computer Science #32 <https://youtu.be/_GzE99AmAQU>

Ethics and principles

The fact that hacker culture is not exclusive to these two subcultures should be noted. Additionally, there is a larger hacker culture that includes people who have a passion for experimenting with technology, pushing the envelope, and encouraging a team-based and imaginative approach to problem-solving. Intellectual curiosity, information freedom, and knowledge exchange are valued in this society. People can take part in endeavours like open-source software creation, hacking contests, and discussion forums within the larger hacker culture.

Cybersecurity has been significantly impacted by hacker culture, which has sparked innovation and advanced defence methods. Hacker conferences like DEF CON and Black Hat, which provide venues for knowledge exchange, the presentation of research, and community interaction, have been affected by the culture.

The ethics and values that underpin the hacking community's behaviour and actions are referred to as hacker culture. There are some universal ethical norms and principles that are frequently linked with hacker culture, despite the fact that it is diverse and can differ among individuals. The hacker ethics are the foundation for many of the beliefs and principles of the free and open source software movement. Steven Levy described hacker ethics in Hackers: Heroes of the Computer Revolution and in other works, where he formulated and enumerated common hacker views.

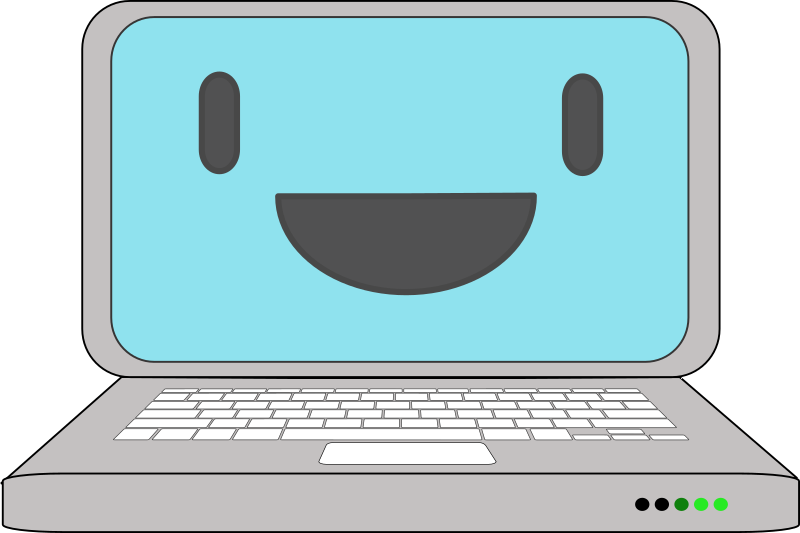
* There should be complete and unrestricted access to computers and everything else that could instruct you on how the world operates.
* Everything should be available for free.
* Hackers should be assessed on their hacking, not on fictitious standards like educational background, age, race, or status.
* On a computer, you can produce beautiful things.
* Your life can improve thanks to computers.

History and timeline

Here is a short informative video about the history and timeline of cybersecurity and hacking:

**Viedo**: A Brief History of Cybersecurity and Hacking, CyberNews, YouTube.com: [A Brief History of Cybersecurity and Hacking](https://youtu.be/V6p7lFsokXo)

Overview of some famous hackers/ groups/ hacks/ viruses (up to 10)



Images source: <https://openclipart.org/detail/204065/evil-computer-laptop>; <https://openclipart.org/detail/204064/happy-computer-laptop>; <https://openclipart.org/detail/201518/sad-laptop>

Here are a few incidents that mark turning points in the history of hacking and cybersecurity, helping to create security procedures, shape policy debates, and raise public awareness of the always expanding threats in the digital sphere. It is not possible to cover all of them and if you are interested you could browse the plethora of information available on the internet and in different forums.

**The Morris Worm:** It is one of the first significant examples of a self-replicating computer worm, and it was developed by Robert Tappan Morris in 1988. Thousands of machines were infected as it spread throughout the early internet. The incident exposed the flaws in networked systems and spurred important developments in cybersecurity techniques, resulting in the formation of groups like CERT and raised awareness of the significance of preventative security measures.

**Operation Aurora (2009):** In 2009, prominent technological corporations, including Google, were the target of a number of cyberattacks under the name Operation Aurora. The attacks, which have been linked to state-sponsored hackers, took advantage of zero-day flaws in well-known software to obtain illegal access and steal intellectual property. This incident highlighted the necessity for strong defences against targeted assaults and the increasing sophistication of advanced persistent threats (APTs).

**Stuxnet (2010):** In 2010, researchers found Stuxnet, a highly sophisticated computer worm that deliberately targeted industrial control systems used in Iran's nuclear program. It is thought that Israel and the United States worked together on it. Stuxnet demonstrated the capability of cyber weapons to physically harm crucial infrastructure and emphasised the significance of safeguarding industrial control systems from cutting-edge cyberthreats.

**WannaCry Ransomware Attack (2017):** In 2017, hundreds of thousands of computers around the world were infected by the WannaCry ransomware attack. The ransomware spread quickly via a flaw in Microsoft Windows, encrypting files, and requesting Bitcoin ransom payments. This incident highlighted the need for prompt patching, reliable backups, and proactive cybersecurity steps to reduce such risks and showed how pervasive the effects of ransomware attacks can be.

**SolarWinds Supply Chain Attack (2020):** In December 2020, a highly sophisticated cyber espionage operation known as the SolarWinds supply chain attack was uncovered. The SolarWinds Orion software, which was utilised by various businesses and government bodies, was compromised. The attackers created a backdoor in the software that gave them access to networks and allowed them to steal sensitive data. This incident brought to light the dangers posed by supply chain intrusions and the requirement for increased examination of third-party providers and software.

### **Conclusions**

The history of hacking has had a significant and wide-ranging influence on society, technology, and security procedures. Significant events have shown weaknesses in networked systems, underscoring the crucial relevance of cybersecurity, from the earliest exploitation motivated by curiosity to sophisticated state-sponsored cyberattacks. These occurrences have led to improvements in defence systems, international conversations on privacy and data protection, and increased collaboration between public and private organisations. Hacking has an effect on geopolitics, national security, and the economy in addition to technology. Knowing this history highlights the importance of constant watchfulness, cooperation, and investment in cybersecurity to maintain a safe and secure digital future.

## **1.4 Operating Systems**

Definition and brief history

An operating system (OS) is a type of system software that controls the resources of a computer, including its hardware and software, and offers standard services to computer programs.It serves as a bridge between people, software, and computer hardware, allowing for quick and regulated access to system resources. Process management, memory management, file system management, device management, and user interface management are among an operating system's core duties.

**History**

Operating systems have a long history that begins with the invention of computers. Computers were bulky, expensive devices run by a group of specialists in the 1950s and 1960s. They were frequently committed to managing just one project or program at a time. When they first emerged, operating systems were merely a thin layer of software that aided in user-hardware communication.

More complex operating systems were required as computers became more potent and diverse. Multiple users may interact with a computer at once thanks to the introduction of time-sharing systems in the late 1960s and early 1970s. Due to the operating system's ability to manage and switch between numerous activities or processes, the idea of multitasking was born.

There were numerous significant operating systems that appeared in the 1970s. The Unix operating system was created by Bell Labs and is now widely used in academic and research settings. With the introduction of fundamental ideas like file system hierarchy, inter-process communication, and a modular structure, Unix became far more scalable and versatile.

Operating system development made tremendous strides during the 1990s. When Microsoft debuted Windows 95, it signalled a change toward computing that was focused on consumers and gave everyone access to a more user-friendly GUI. As a result of their reliability, security, and open-source nature, numerous Unix varieties, including Linux, gained popularity concurrently, especially in the server and enterprise space.

GNU/Linux

GNU is a Unix-like operating system. That indicates that it is a collection of numerous programs, including games, libraries, developer tools, and apps. The GNU Project began in January 1984. There are numerous GNU programs—known as GNU packages— which are made available for download under the GNU Project's aegis.

An open-source operating system called GNU/Linux combines the Linux kernel with the GNU userland utilities. Due to its dependability, security, adaptability, and capacity for system customization and modification to meet specific demands, it has grown incredibly popular. Here, we'll talk about some important features of GNU/Linux, such as the file system, users and groups, services, and fundamental commands.

List of GNU Core Utilities commands could be found here: <https://en.wikipedia.org/wiki/List_of_GNU_Core_Utilities_commands>

Click on the links to read more information about the following topics:

Users and groups information

<https://www.gnu.org/software/libc/manual/html_node/Users-and-Groups.html>

Services

<https://guix.gnu.org/manual/en/html_node/Services.html>

File system

<https://opensource.com/life/16/10/introduction-linux-filesystems>

## Windows

One of the most popular and well-known operating systems in the world is the Windows operating system, created by Microsoft. Windows, which is renowned for its user-friendly interface, has developed over many years to offer a complete platform for personal computers and servers. Windows has improved performance, added new features, and enhanced compatibility with a wide variety of hardware and software with each new release. Users of all technical proficiency levels can utilise it thanks to its simple graphical user interface (GUI). Windows is a staple of productivity, gaming, and entertainment and supports a large number of apps. Windows continues to dominate the operating system industry, whether it is used for personal, academic, or professional purposes. It powers millions of devices and offers a robust ecosystem of apps and services.

List of Windows Core Utilities commands could be found here

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/windows-commands>

Users and groups information

<https://www.digitalcitizen.life/geeks-way-managing-user-accounts-and-groups/>

Services

<https://learn.microsoft.com/en-us/dotnet/framework/windows-services/introduction-to-windows-service-applications>

File system

<https://learn.microsoft.com/en-us/troubleshoot/windows-client/backup-and-storage/fat-hpfs-and-ntfs-file-systems>

OS components

The operating system's components are all necessary to ensure that a computer's many components communicate with one another. To use any hardware, whether it be as basic as a mouse or keyboard or as complicated as an Internet component, all user software must pass via the operating system.

**Kernel**

The central element of an operating system is the kernel. It is in charge of overseeing system resources like memory, the CPU, and input and output devices. The kernel acts as a link between software programs and the underlying hardware by providing necessary services and interfaces for other parts.

**File System**

On storage devices such hard drives, solid-state drives, or flash drives, the file system is in charge of managing the files and directories. In addition to preserving metadata, rights, and access control, it offers ways to create, read, write, and delete files.

**Device Drivers**

Device drivers let the operating system and hardware components like printers, network adapters, and graphics cards communicate with one another. They offer an interface through which the operating system can communicate with particular hardware parts and regulate their operation.

**User Interface**

Users can communicate with the operating system and its applications through the user interface. It can be graphical (GUI), which offers a visual environment with icons, windows, and menus for intuitive interaction, or command-line based (CLI), where users type text commands.

**Process Management**

Creating, planning, and ending computer processes or programs are all part of process management. The operating system provides methods for interprocess communication and synchronisation as well as resource allocation and execution management for processes.

**Memory Management**

The system's memory resources are allocated and reallocated by memory management. It controls virtual memory, makes sure that the memory that is available is used effectively, and offers means for protecting and sharing memory among processes.

**Networking**

Computers may communicate and share resources via a network thanks to networking components that let the operating system create and manage network connections. This comprises the networking stacks, drivers, and protocols responsible for data transmission, routing, and network security.

**Videos:**

Operating Systems: Crash Course Computer Science #18 <https://youtu.be/26QPDBe-NB8>

Memory & Storage: Crash Course Computer Science #19 <https://youtu.be/TQCr9RV7twk>

Files & File Systems: Crash Course Computer Science #20 <https://youtu.be/KN8YgJnShPM>

Graphical User Interfaces: Crash Course Computer Science #26 <https://youtu.be/XIGSJshYb90>

Security of OS

In today's networked world, OS security is of utmost importance. An OS is a target for cyberattacks because it provides the framework for managing system resources and operating programs. Implementing numerous safeguards to guard against unwanted access, data breaches, and system vulnerabilities is necessary to ensure an OS's security. This consists of strong user authentication systems, secure communication protocols, access restrictions, encryption, and frequent security updates. OS security also entails keeping an eye on and auditing system activity, identifying and thwarting security risks, and preserving the OS's integrity by using tools like malware detection and eradication. As part of the broader cybersecurity initiatives, a secure OS is essential for safeguarding sensitive data, preserving privacy and preserving the stability and reliability of computer systems.

### **Conclusions**

In conclusion, having a secure OS is crucial. A secure OS safeguards confidential data, protects against intrusions and guarantees the reliability and security of a computer system. A secure OS also reduces the risks and maintains the protection of data by putting in place robust security mechanisms, such as access controls and regular upgrades. It is a very important component of a comprehensive cybersecurity strategy, which fosters user confidence and promotes a secure digital environment.

## **1.5 Networking**

## Definition

Networking in the context of IT refers to the act of connecting together various hardware and software in order to simplify the sharing of data and resources. Computers, servers, printers, and other network-capable devices can connect and share data with one another thanks to networking. In order to establish connections and permit data transfer, it entails the use of hardware devices like routers, switches, and modems as well as networking protocols and technologies. Users can communicate via email, texting, video conferencing, and internet access while using networking to access shared resources like files and printers. In today's IT infrastructure, it is essential for facilitating resource access, collaboration, and communication across local and wide-area networks.

Wired networking and wireless networking are the two main categories of computer networking. In wired networking, data must be transferred between nodes through a physical medium. Due to its low cost and dependability, copper-based Ethernet cable is frequently utilised in households and companies for digital communications. As an alternative, optical fibre is utilised to move data farther and quicker, but it comes with a number of drawbacks, such as higher costs and more delicate parts.

Devices can connect to a network wirelessly by using radio waves to transmit data over the air, doing away with the need for cables. The most popular and commonly used type of wireless networking is wireless local area networks (LANs). Microwave, satellite, cellphone, and Bluetooth are a few alternatives. In general, wired networking is faster, more dependable, and more secure than wireless networks, which typically offer better adaptability, mobility, and scalability.

## Key components

Physical network infrastructure, such as switches, routers, and wireless access points, as well as the underlying firmware that runs such hardware are needed for computer networking. The software required to manage, secure, and monitor the network is among the other components.

Network Devices: These are hardware devices that facilitate network connectivity and data transfer. Common network devices include routers, switches, modems, network interface cards (NICs), access points, and firewalls.

Network Cables: Physical cables, such as Ethernet cables, fiber optic cables, or coaxial cables, are used to establish wired connections between devices in a network. These cables transmit data signals between devices.

Network Topology: Network topology refers to the physical or logical layout of devices and connections in a network. Common network topologies include star, bus, ring, mesh, and hybrid topologies.

IP Addressing: IP addressing is the system used to assign unique addresses to devices in a network. IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6) are the two main versions of IP addressing used to identify and locate devices on a network.

Network Security: Network security involves implementing measures to protect the network and its data from unauthorised access, attacks, and vulnerabilities. This includes using firewalls, VPNs (Virtual Private Networks), encryption, authentication mechanisms, and intrusion detection and prevention systems.

Furthermore, regardless of the underlying technology, networks rely on the adoption of standard protocols to consistently perform distinct functions or convey different types of data.

## Internet protocol suite

The Internet Protocol Suite, also known as the TCP/IP (Transmission Control Protocol/Internet Protocol) suite, is a collection of networking protocols and standards that enable communication and data transfer over the internet. It provides a comprehensive framework for reliable and secure transmission of data between devices connected to different networks.

Four sorts of data transmission layers are categorised by the TCP/IP model. The application layer, transport layer, internet layer, and data link layer are among these four layers. Basically, it involves tracking a packet's complete path, from the moment you request a page in your browser to the point at which the web server responds and renders the page's contents.

Application layer

The portion of the computer network that is visible is called the application layer. It covers all of the protocols, as well as the interactive web apps, email, and other programs we use online.

Transport layer

The packaging of data, including its construction and deconstruction into data packets for network transmission, falls within the purview of the transport layer. To send and receive data, the transport layer relies on the internet layer's routing and delivery capabilities.

Internet layer

Data packets are sent, routed, and received over the network by the internet layer.

Data link layer

The physical characteristics of the network, including the NIC card, ethernet cables, fiber link, and all other hardware-level components that carry out the actual labor-intensive operation of moving digital data from one location to another via the network, are represented by the data link layer.

| **Layer Name** | **Protocols** |
| --- | --- |
| **Application** | HTTP, FTP, POP3, SMTP, SNMP |
| **Transport** | TCP, UDP |
| **Internet** | IP, ICMP |
| **Data link** | Ethernet, ARP |

## 

## OSI model (the 7 layers)

A conceptual framework known as OSI (Open Systems Interconnection) specifies the many layers involved in network communication. It aids in comprehending and illuminating the interactions between various network protocols and technologies. Seven levels make up the OSI model, and each has a distinct set of duties:

The OSI model, image source: <https://openclipart.org/detail/295502/osilayermodel>

7. Application Layer: The topmost layer, the application layer engages with user applications directly. It offers protocols and services for network applications like file transfers, email, and web browsing. The HTTP, SMTP, FTP, and DNS protocols are a few examples of application layer protocols.

6. Presentation layer: Data representation, encryption, compression, and formatting are all handled by the presentation layer. It makes sure that information transmitted by the application layer is correctly formatted and is comprehensible by the program receiving it.

5. Session layer:Establishing, managing, and ending communication sessions between apps is done by the session layer. It offers solutions for session creation, synchronisation, and checkpointing.

4. Transport Layer: The transport layer makes sure that data is sent between hosts in an effective and dependable manner. It creates connections, handles flow management, divides data into smaller parts, and offers techniques for error recovery. At the transport layer, TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) function.

3. Network layer: The network layer is in charge of logical addressing and data packet routing across various networks. It chooses the most efficient route for data transmission, handles routing, and controls IP addressing. Network layer protocols include the Internet Protocol (IP).

2. Data Link Layer: The data link layer ensures that data frames are sent between network nodes without mistake. It manages media access management, error detection and repair, and data framing. An illustration of a data link layer protocol is Ethernet.

1. Physical Layer: The OSI model's bottom layer, it deals with the actual physical transport of data through networks. It outlines the network's physical, mechanical, and electrical properties, such as its cables, connectors, and signalling.

In order to enable network communication, each layer in the OSI model carries out certain tasks and engages in interactions with the layers above it. The model aids in network design and debugging, as well as in comprehending data flow and the function of various protocols at each layer.

### **Conclusions**

Networking is a crucial component of contemporary technology and communication. It makes it possible for people, organisations, and gadgets all over the world to connect and exchange information, resources, and ideas with ease. Collaboration is made easier by networking, which also increases output and gives access to beneficial possibilities and resources. In today's interconnected world, networking is essential for facilitating seamless communication, promoting creativity, and accelerating growth, whether it be for personal, professional, or organisational reasons.

## 

## **1.6 System Administration**

## The management and upkeep of servers, networks, and computer systems within a company are referred to as system administration. System administrators, also referred to as sysadmins, are in charge of making sure that the company's IT infrastructure runs efficiently and is secure and dependable. Their main responsibilities include setting up operating systems and software, managing user accounts and access rights, keeping an eye on system performance, troubleshooting problems, putting security measures in place, and performing routine backups and system updates.

## System administrators are essential to a company's capacity to provide IT services with integrity and availability. To satisfy the organisation's technological needs, deal with technical difficulties, and assist end users, they collaborate closely with other IT specialists and departments. Strong technical expertise, problem-solving abilities, and the capacity for technological evolution are requirements for system management.

Here is how the GNU/Linux and Windows systems administrations differ.

## GNU/Linux

# To get you started you could read this: Bash Scripting Tutorial – Linux Shell Script and Command Line for Beginners: <https://www.freecodecamp.org/news/bash-scripting-tutorial-linux-shell-script-and-command-line-for-beginners/>

You can view this Linux System administrator course:

<https://youtu.be/UCr04qIB7uc>

## Windows

What is PowerShell:

<https://learn.microsoft.com/en-us/powershell/>

# Windows Powershell vs Command Prompt: What's The Difference Anyway? <https://youtu.be/H0gwnFV_SFs>

# Introduction to scripting in PowerShell: <https://learn.microsoft.com/en-us/training/modules/script-with-powershell/>

### **Conclusions**

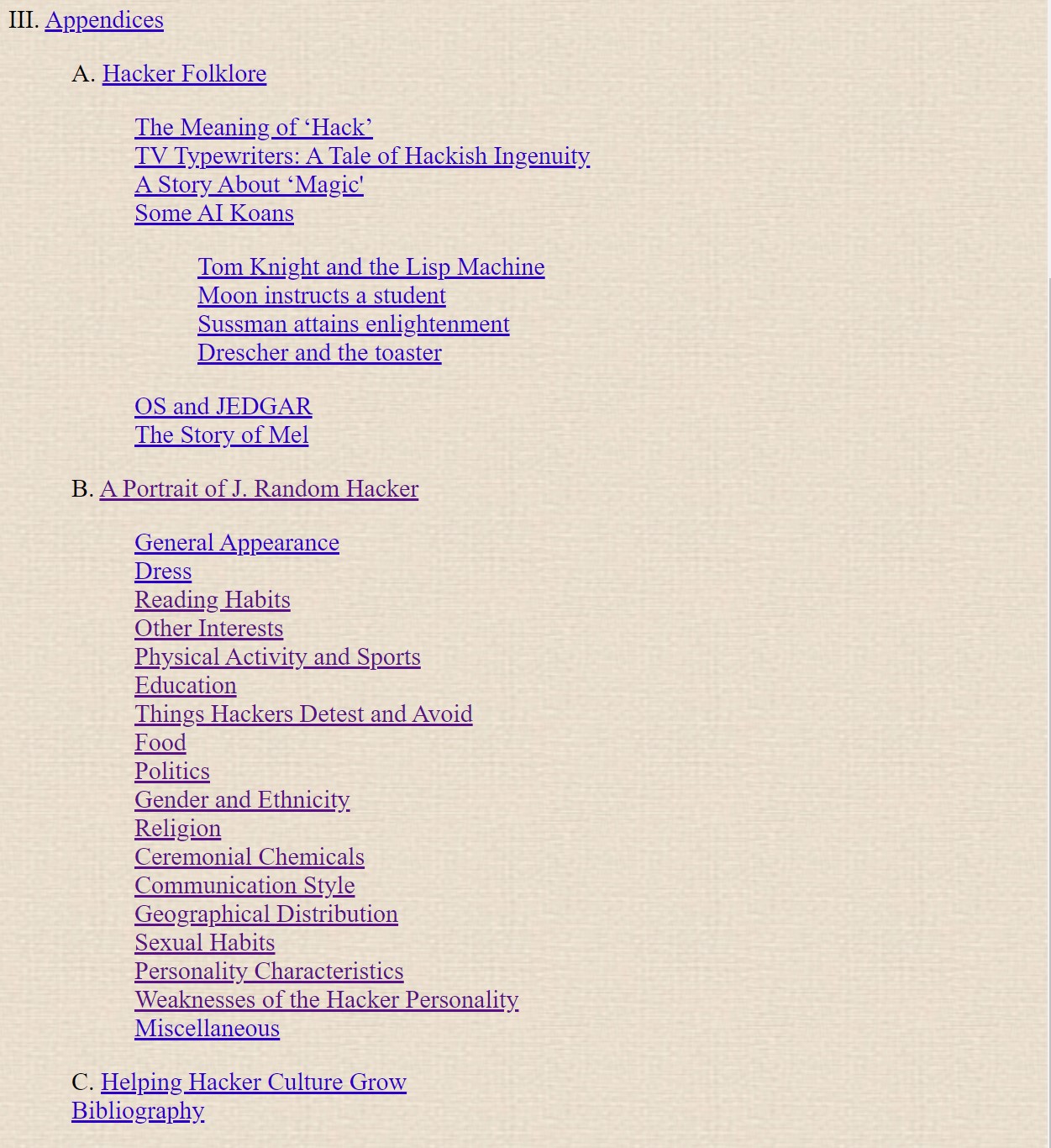
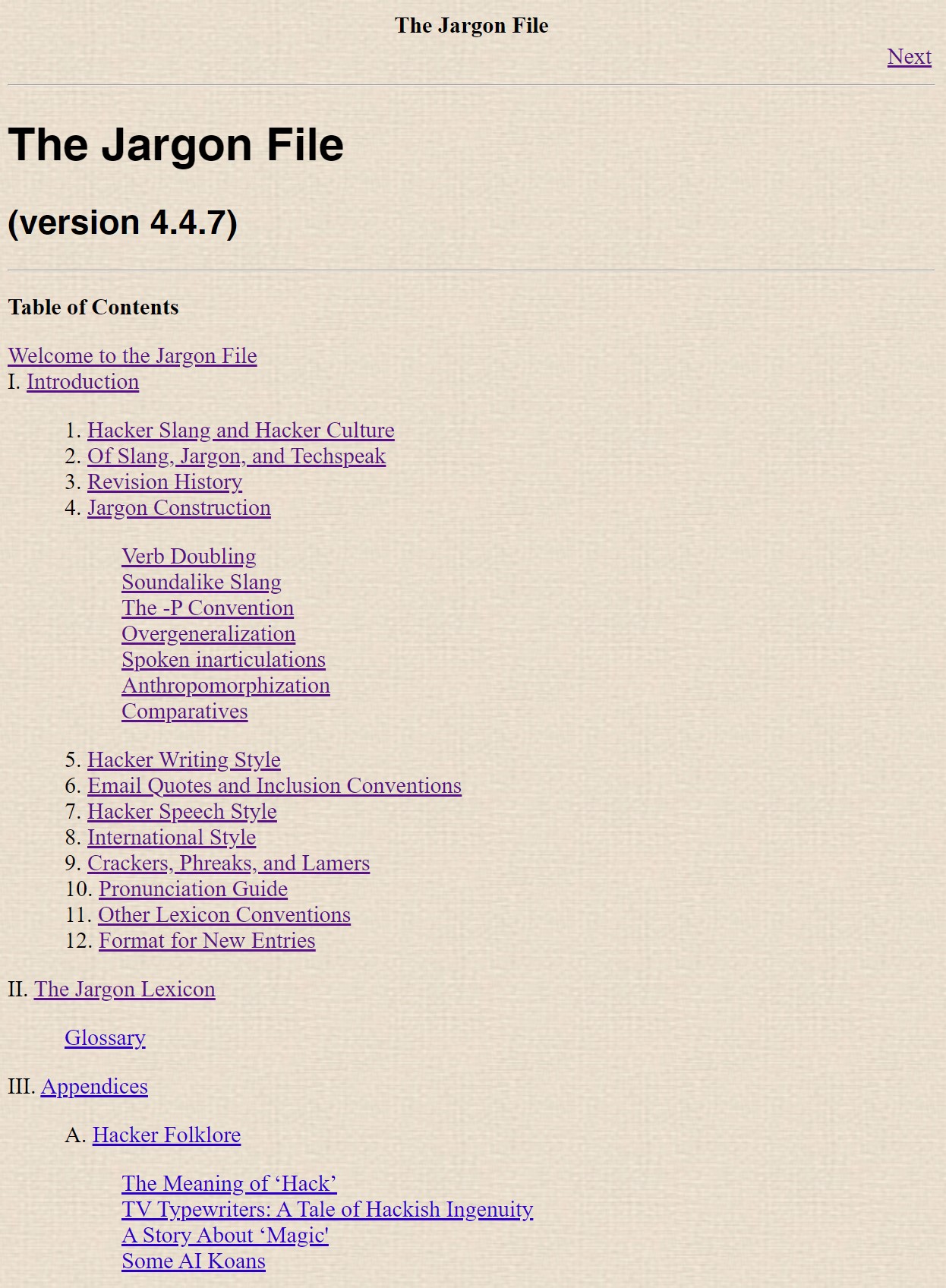
In general GNU/Linux offers greater flexibility, allowing administrators to tailor the system to specific requirements. It is widely used in server environments, providing a foundation for various applications and services. Windows focuses on ease of use and compatibility, making it popular for desktop systems. Last but not least GNU/Linux is typically free and open-source, making it an attractive option for organisations with budget constraints. Windows involves licensing costs, but it also provides commercial support and compatibility advantages for specific applications and hardware.open source and free. Both systems offer a lot of options and services and are worth exploring in depth.

## 

## **1.7 The *Jargon File***

What the Jargon file is

The Jargon File, also known as the hacker's dictionary, is a comprehensive glossary of technical jargon, slang, and terms related to computing, hacking, and the hacker culture. Originally started by Raphael Finkel in 1975, it has been maintained and expanded by the hacker and computer enthusiast community over the years. The Jargon File provides insights into the history, ethos, and terminology of hacker and programmer subcultures, offering explanations and humorous anecdotes for various terms. It aims to bridge the communication gap between technical insiders and outsiders, making it easier for non-experts to understand and participate in discussions related to computing and technology.



You can review the Jargon file by yourself here: <http://catb.org/jargon/html/online-preface.html>

## **The Geek’s Corner**

**Sc.exe**

Windows operating systems come with a command-line program called sc.exe (Service Control) that makes it possible to control and configure Windows services. On a local or remote computer, it gives administrators the power to build, change, query, start, stop, and delete services. Administrators are able to automate service-related actions and set service settings thanks to the sc.exe utility's interaction with the Service Control Manager (SCM).

Administrators can manage Windows services in a number of ways with sc.exe. They have the ability to establish new services, defining the startup options as well as the executable or command that the service will use to run. Using the utility, service configurations can be changed, including the display names, descriptions, and dependencies of the services. Additionally, administrators have the ability to initiate, stop, and delete services as needed. They may also query the status and characteristics of already-running services. All things considered, sc.exe is a flexible tool for effectively controlling Windows services from the command line, giving administrators fine-grained control over the services active on their systems.

Read more about the:

sc.exe config

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/sc-config>

sc.exe create

[http00s://learn.microsoft.com/en-us/windows-server/administration/windows-commands/sc-create](https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/sc-create)

sc.exe delete

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/sc-delete>

sc.exe query

<https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/sc-query>

# **Conclusions**

This was our brief overview of the core principles of cyber security. This unit on cybersecurity basics covered the basics of the core principles in the field. We have explored information security, the fundamental principles of cybersecurity, and the significance of the CIA standard. Additionally, we have looked into the history and best practices of the CIA triad, examined aspects of the hacker culture, and gained some insights into operating systems, networking, and system administration. The field, however, is a lot more vast and complex than what we can cover here and there is a lot more to explore if you are interested.

## 

## **Quiz**

**1 What does the CIA standard refer to in the context of information security?**

A) A framework for assessing the financial impact of security breaches.

**B) A set of principles that ensure confidentiality, integrity, and availability of information.**

C) A protocol used for securing wireless network communications.

D) A standard for encryption algorithms used in secure communication protocols.

**2 What is hacking?**

**A) The act of gaining unauthorised access to computer systems or networks for malicious purposes**

B) A technique used to exploit software vulnerabilities and develop patches or fixes.

C) The process of encrypting sensitive data to ensure secure transmission and storage.

D) The practice of optimising computer systems.

**3 What is an operating system?**

A) The main software that manages computer resources and controls computer operations.

B) The software that enables users to perform tasks and run programs on a computer.

**C) The system software that provides services to applications and manages computer resources.**

D)The hardware component responsible for managing and executing instructions in a computer system.

**4 What is networking in the context of computer science?**

**A) The practice of establishing connections and communication between computers or other devices.**

B) The process of configuring hardware components within a computer system.

C) The development and maintenance of social connections in the technology industry.

D) The implementation of security measures to protect computer networks from unauthorised access.

**5 What does OSI stand for in the context of computer networks?**

A) Open System Integration

B) Operational Security Implementation

**C) Open Systems Interconnection**

D) Optimal System Infrastructure

## 

## **References**

**What Is Information Security? - CISCO** <https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html> [accessed on 03.05.2023]

The early hackers - catb.org

<http://catb.org/~esr/writings/hacker-history/hacker-history-3.html> [accessed on 04.05.2023]

….

The original hacker’s dictionary: <https://www.dourish.com/goodies/jargon.html> [accessed on 04.05.2023]

Bell–LaPadula model: <https://en.wikipedia.org/wiki/Bell%E2%80%93LaPadula_model> [14.06.2023]

Information security: <https://en.wikipedia.org/wiki/Information_security#Key_concepts>

[14.06.2023]

A brief history of hacking: <https://encyclopedia.kaspersky.com/knowledge/a-brief-history-of-hacking/> [14.06.2023]

What is GNU? <https://www.gnu.org/home.en.html> [14.06.2023]

Linux and the GNU System <https://www.gnu.org/gnu/linux-and-gnu.html> [14.06.2023]

Networking (computer) <https://www.techtarget.com/searchnetworking/definition/networking> [15.06.2023]

IBM, What are the basic elements of a network? <https://www.ibm.com/docs/en/zos-basic-skills?topic=networks-what-are-basic-elements-network> [15.06.2023]

Internet protocol suite <https://en.wikipedia.org/wiki/Internet_protocol_suite> [15.06.2023]

What is TCP/IP protocol suite? <https://goteleport.com/learn/what-is-tcp-ip-protocol-suite/> [15.06.2023]

OSI model <https://en.wikipedia.org/wiki/OSI_model> [15.06.2023]

The Jargon File <http://catb.org/jargon/html/online-preface.html> [15.06.2023]