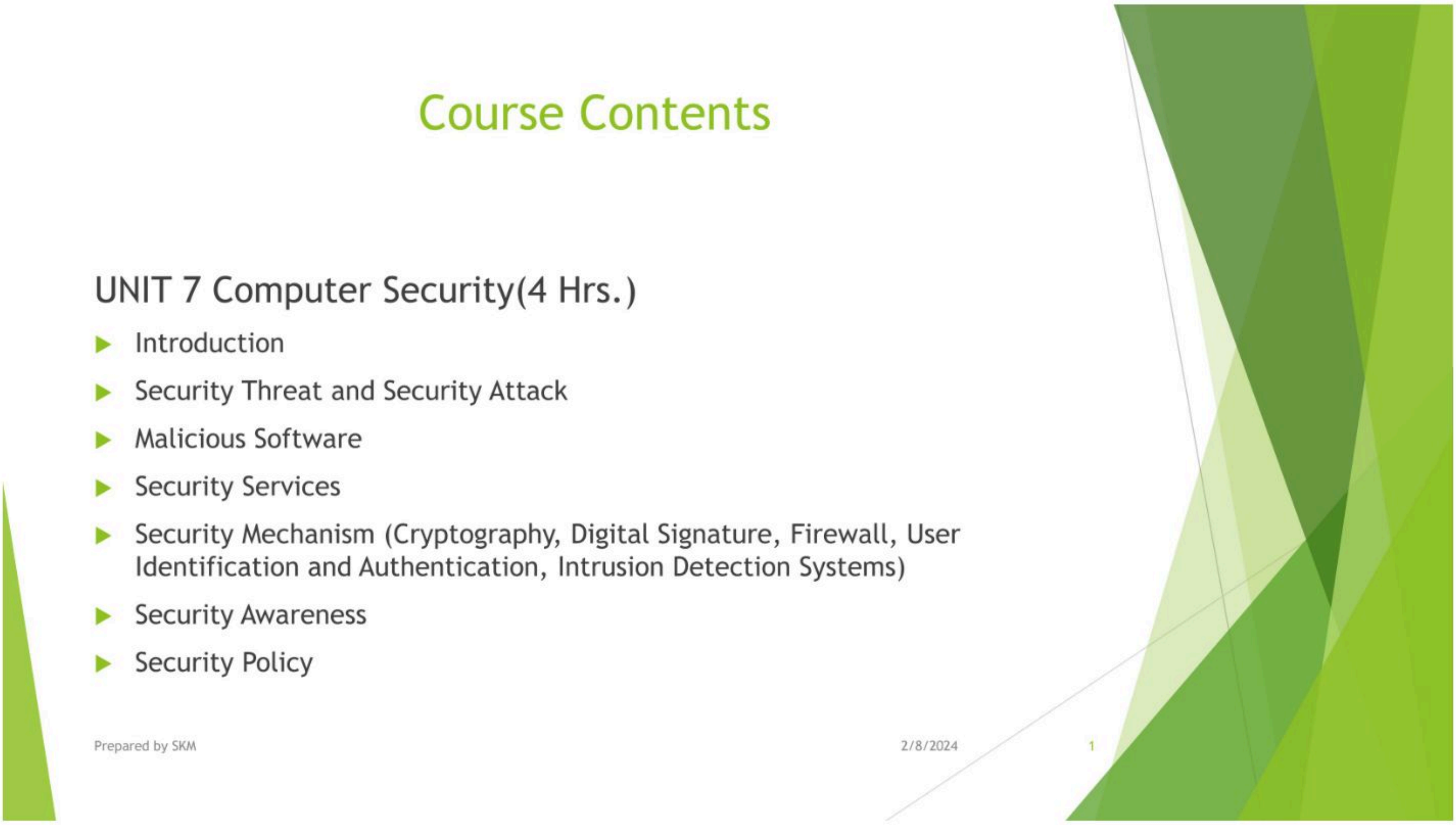


Course Contents

UNIT 7 Computer Security(4 Hrs.)

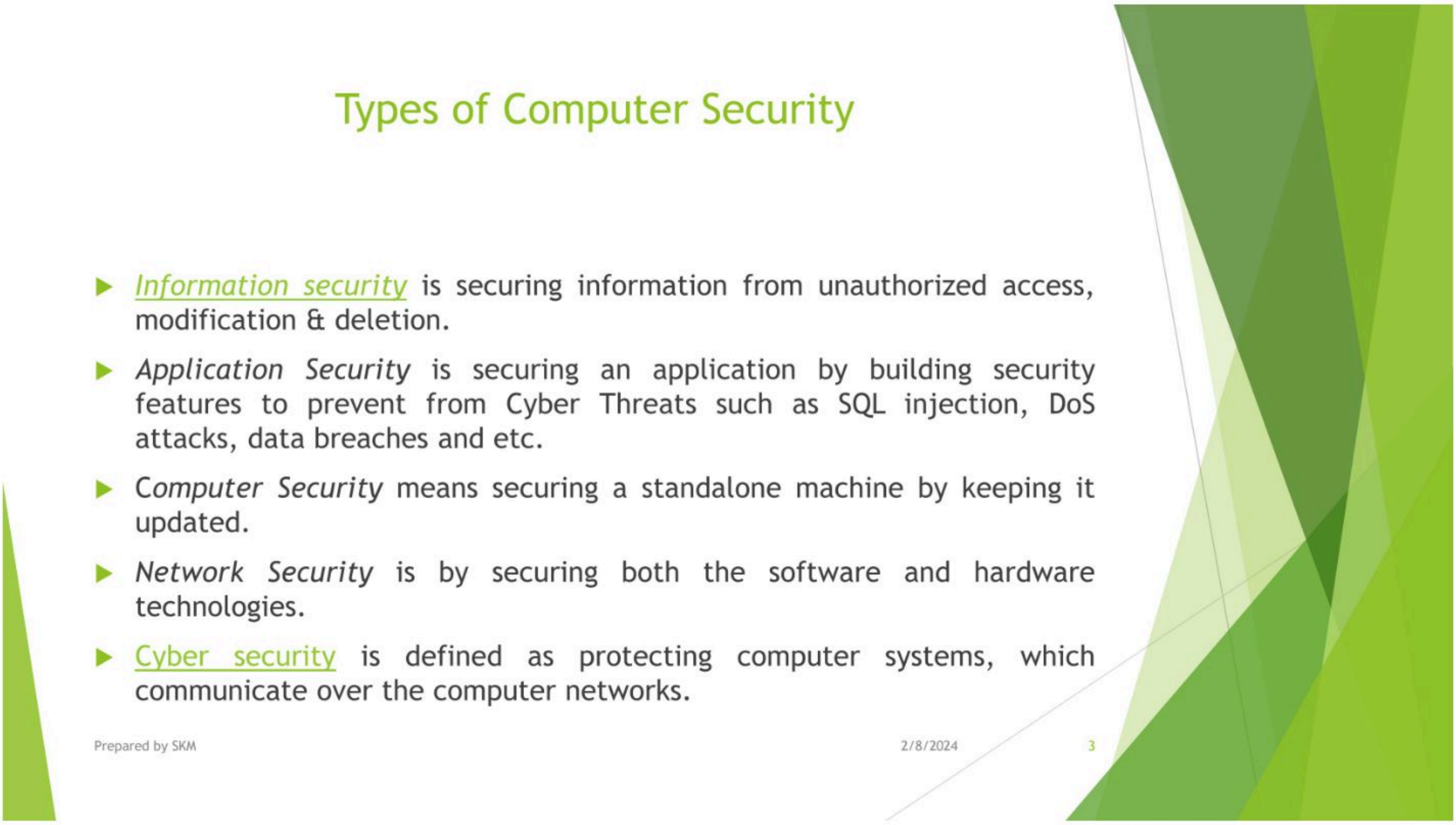
- Introduction
- Security Threat and Security Attack
- Malicious Software
- Security Services
- Security Mechanism (Cryptography, Digital Signature, Firewall, User Identification and Authentication, Intrusion Detection Systems)
- Security Awareness
- Security Policy

Scanned By Camera Scanner

Introduction to Computer Security

- Computer security basically is the protection of computer systems and information from harm, theft and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.
- There are various types of computer security which is widely used to protect the valuable information of an organization.

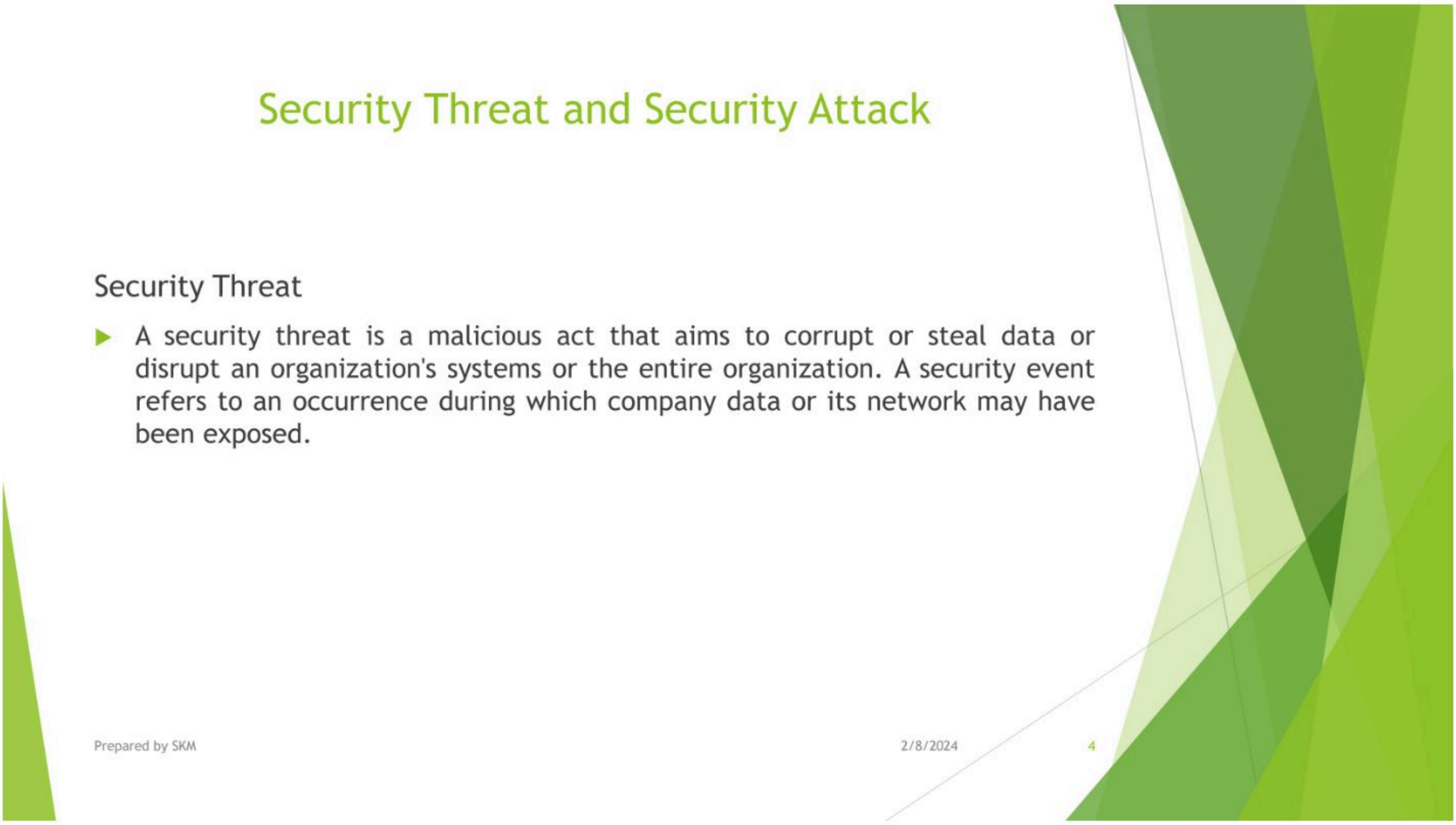
Scanned By Camera Scanner



Types of Computer Security

- *Information security* is securing information from unauthorized access, modification & deletion.
- *Application Security* is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.
- *Computer Security* means securing a standalone machine by keeping it updated.
- *Network Security* is by securing both the software and hardware technologies.
- Cyber security is defined as protecting computer systems, which communicate over the computer networks.

Scanned By Camera Scanner



Security Threat and Security Attack

Security Threat

- A security threat is a malicious act that aims to corrupt or steal data or disrupt an organization's systems or the entire organization. A security event refers to an occurrence during which company data or its network may have been exposed.

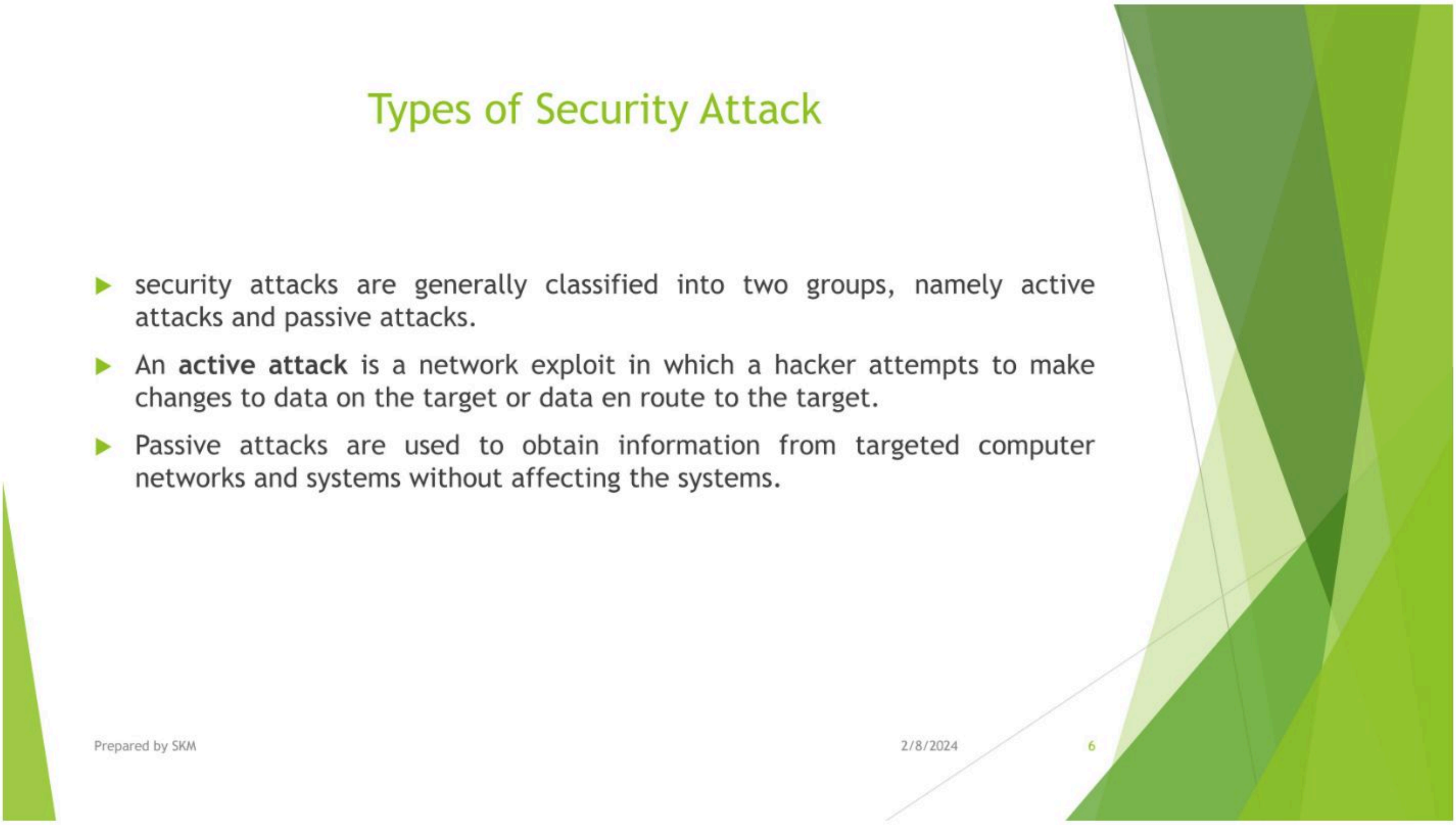
Scanned By Camera Scanner

Security Threat and Security Attack

Security Attack

- An attempt to gain unauthorized access to information resource or services, or to cause harm or damage to information systems.
- Any action that compromises the security of information owned by an organization.

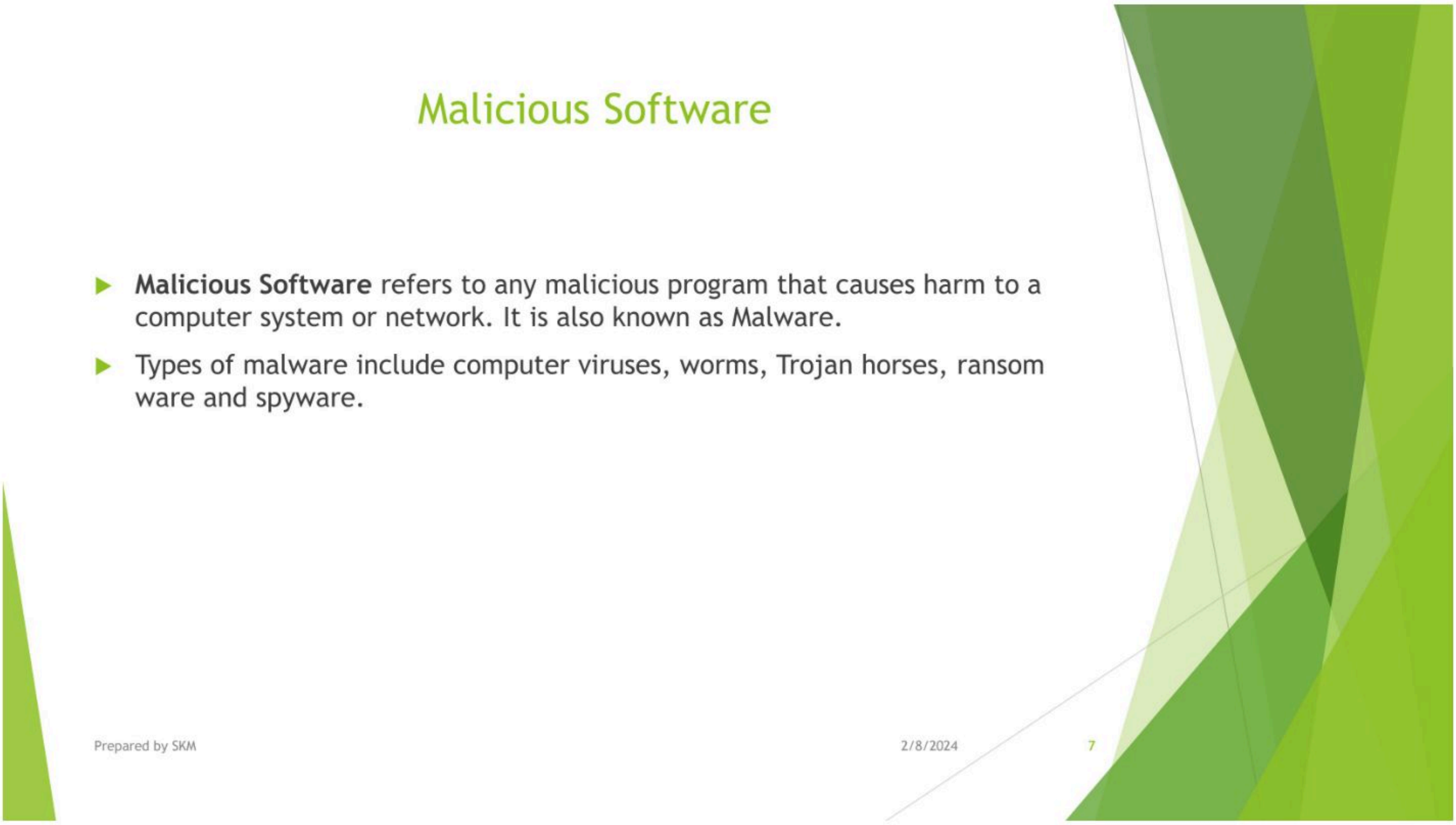
Scanned By Camera Scanner



Types of Security Attack

- security attacks are generally classified into two groups, namely active attacks and passive attacks.
- An **active attack** is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target.
- Passive attacks are used to obtain information from targeted computer networks and systems without affecting the systems.

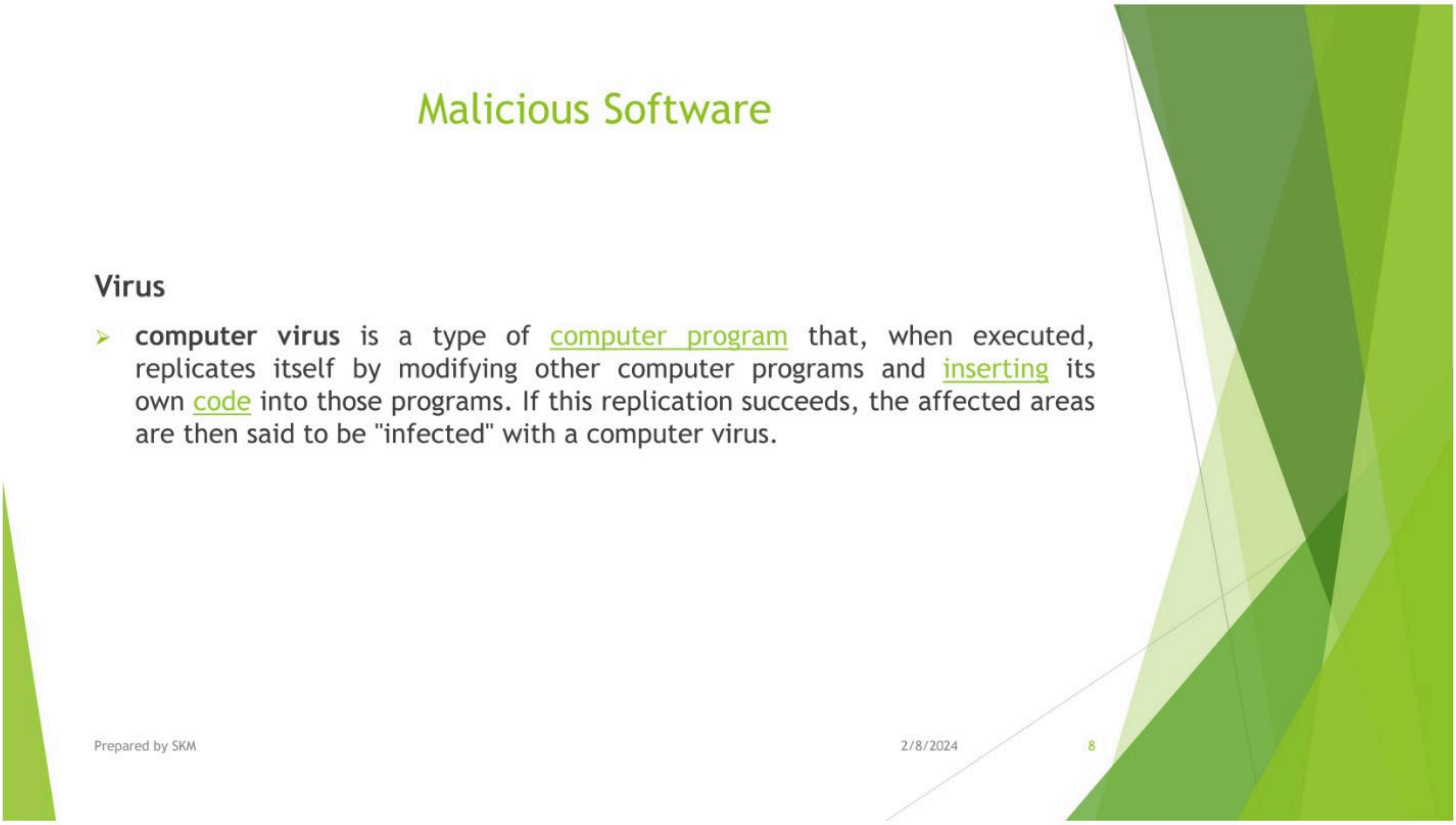
Scanned By Camera Scanner



Malicious Software

- **Malicious Software** refers to any malicious program that causes harm to a computer system or network. It is also known as Malware.
- Types of malware include computer viruses, worms, Trojan horses, ransom ware and spyware.

Scanned By Camera Scanner

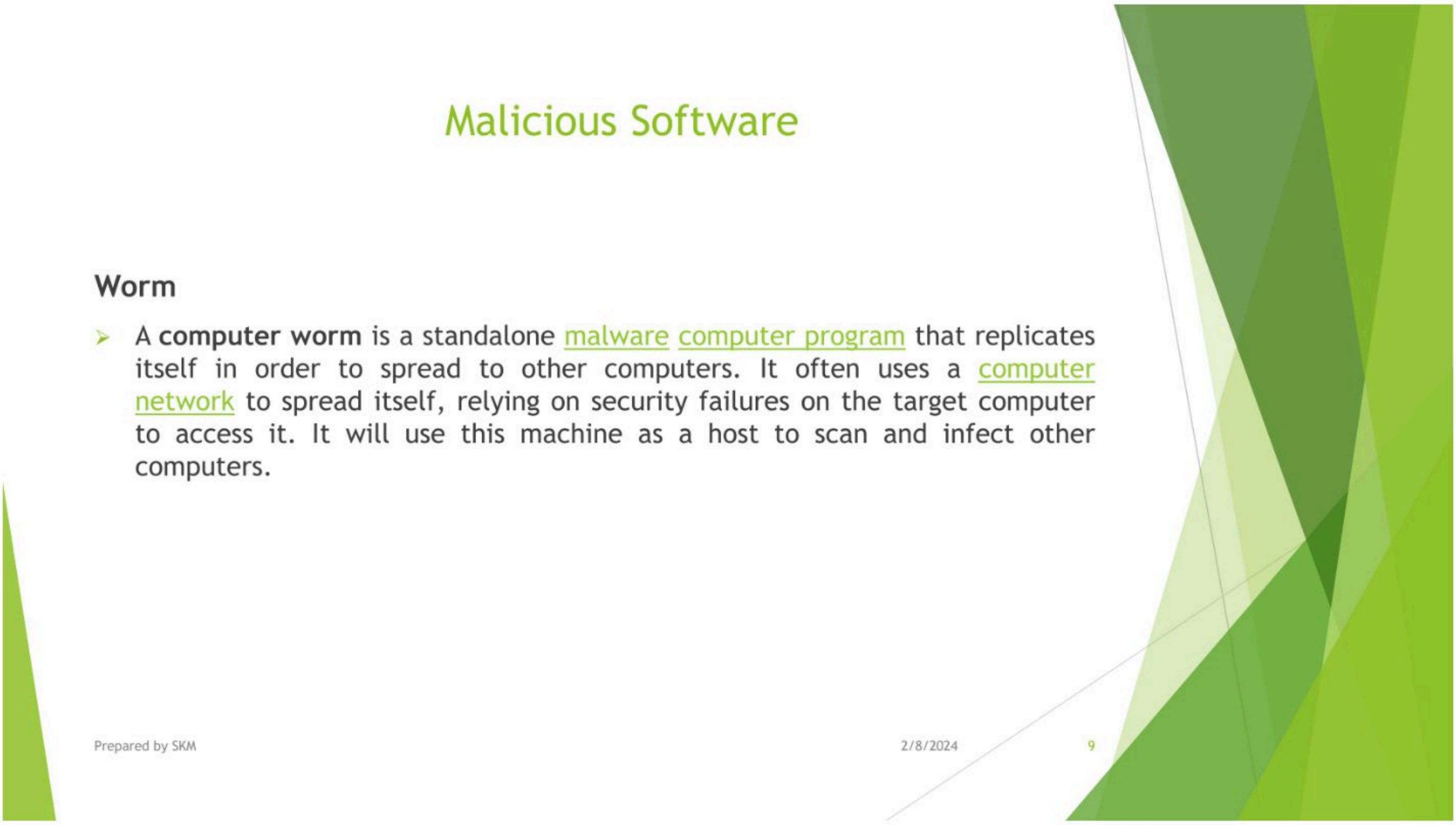


Malicious Software

Virus

- **computer virus** is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

Scanned By Camera Scanner

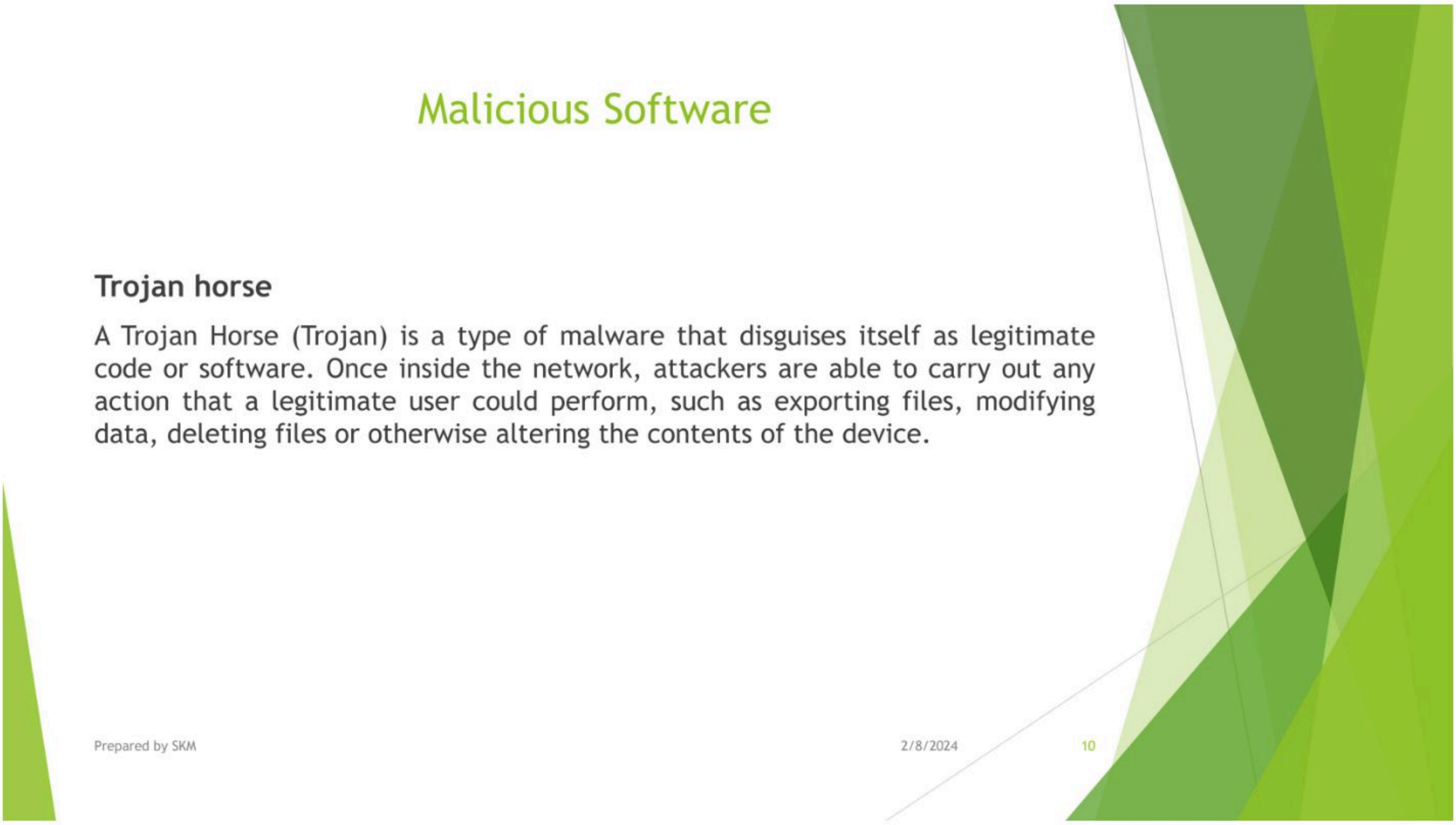


Malicious Software

Worm

- A **computer worm** is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.

Scanned By Camera Scanner



Malicious Software

Trojan horse

A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate code or software. Once inside the network, attackers are able to carry out any action that a legitimate user could perform, such as exporting files, modifying data, deleting files or otherwise altering the contents of the device.

Scanned By Camera Scanner

Malicious Software

Ransomware

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off. While some simple ransomware may lock the system without damaging any files, more advanced malware uses a technique called cryptoviral extortion.

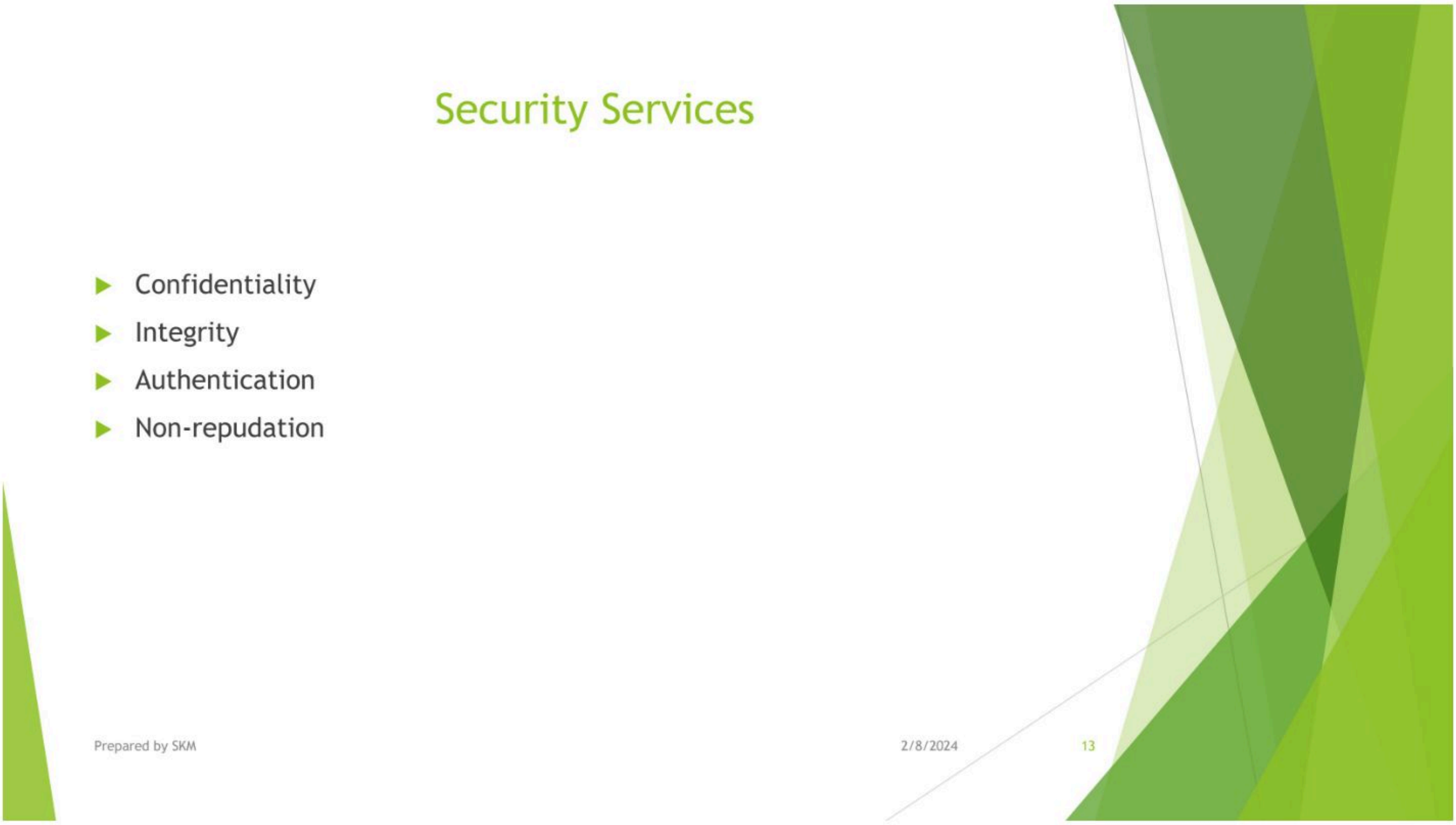
Scanned By Camera Scanner

Malicious Software

Spyware

- Spyware is any software that installs itself on your computer and starts covertly monitoring your online behavior without your knowledge or permission. Spyware is a kind of malware that secretly gathers information about a person or organization and relays this data to other parties.

Scanned By Camera Scanner



Security Services

- Confidentiality
- Integrity
- Authentication
- Non-repudation

Scanned By Camera Scanner

Security Services

Confidentality

- The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- intended for or restricted to the use of a particular person, group, or class : private, secret.
- confidential information. : containing information whose unauthorized disclosure could be prejudicial to the national interest compare secret, top secret. : marked by intimacy or willingness to confide. a confidential

Scanned By Camera Scanner

Security Services

Integrity

- The term 'integrity' means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- **Integrity** is the protection of system data from intentional or accidental unauthorized changes.

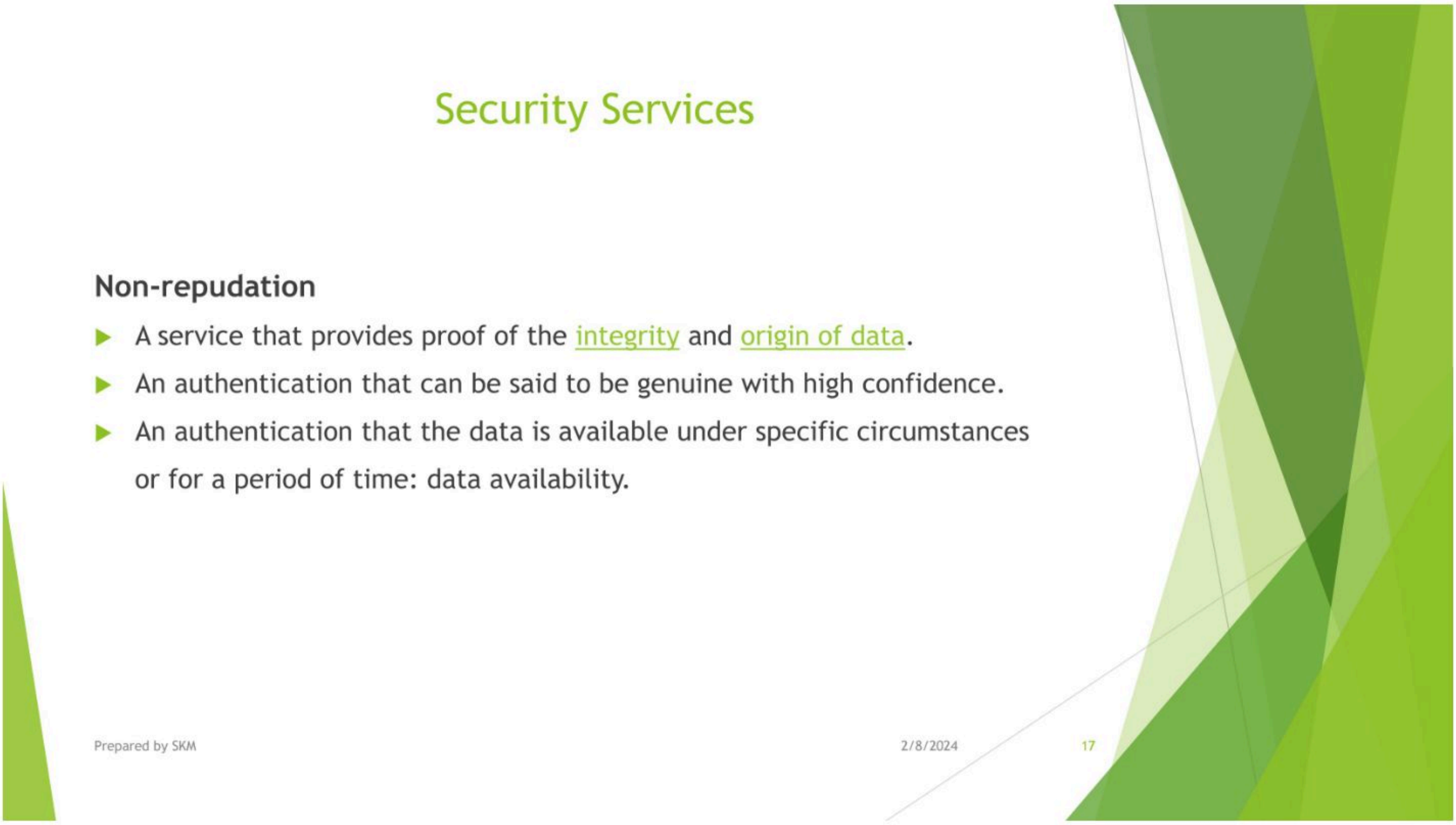
Scanned By Camera Scanner

Security Services

Authentication

- Authentication means verifying whether a user is who they claim to be. On the other hand, authorization means verifying whether a user has privileges to access some data or not. Authentication and authorization are entirely different. One checks for identity, while the other checks access control.

Scanned By Camera Scanner



Security Services

Non-repudiation

- A service that provides proof of the integrity and origin of data.
- An authentication that can be said to be genuine with high confidence.
- An authentication that the data is available under specific circumstances or for a period of time: data availability.

Scanned By Camera Scanner

Security Mechanism

- A mechanism that is designed to detect, prevent, or recover from a security attack. Security Service: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.
- Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service.
- Examples of common security mechanisms are as follows: Cryptography. Message digests and digital signatures.

Scanned By Camera Scanner

Cryptography

- Cryptography is the science of encrypting and decrypting data.
- Cryptography is the art of science.
- Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.
- In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

Scanned By Camera Scanner

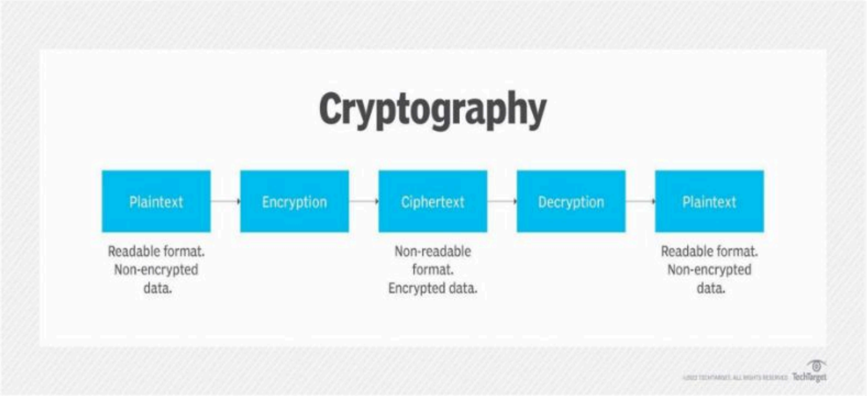
Objectives of Cryptography

Modern cryptography concerns itself with the following four objectives:

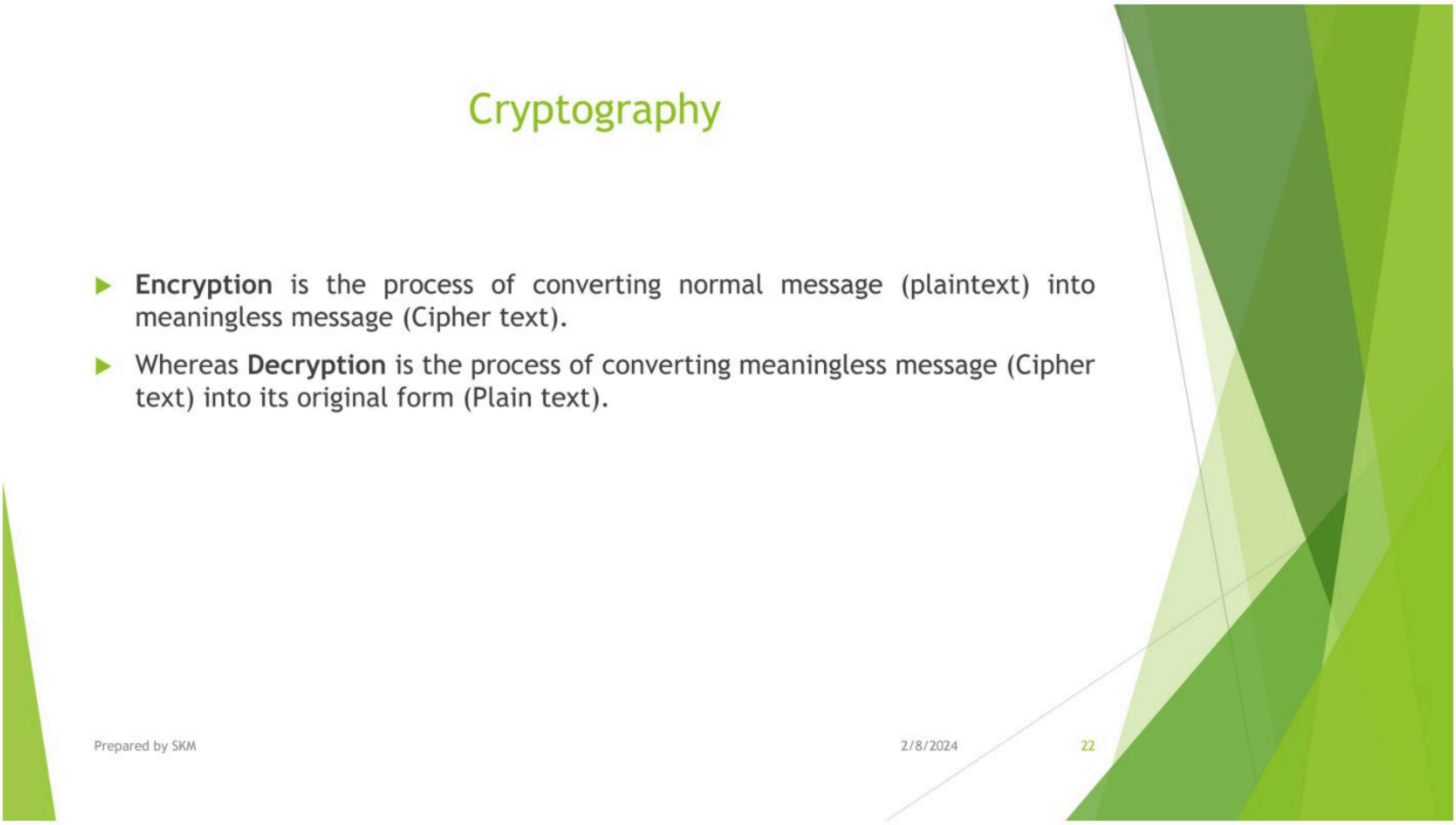
- **Confidentiality.** The information cannot be understood by anyone for whom it was unintended.
- **Integrity.** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
- **Non-repudiation.** The creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.
- **Authentication.** The sender and receiver can confirm each other's identity and the origin/destination of the information.

Scanned By Camera Scanner

Cryptography


Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
©2022 TECHTARGET. ALL RIGHTS RESERVED TechTarget

Scanned By Camera Scanner



Cryptography

- **Encryption** is the process of converting normal message (plaintext) into meaningless message (Cipher text).
- Whereas **Decryption** is the process of converting meaningless message (Cipher text) into its original form (Plain text).

Scanned By Camera Scanner

Introduction to secret key and public key cryptography

- Secret Key is used to both encryption and decryption of the data and the data is shared between the receiver and sender of encrypted data.
- The public key is used to encrypt data and to decrypt the data, the private key is used and is shared.

Scanned By Camera Scanner

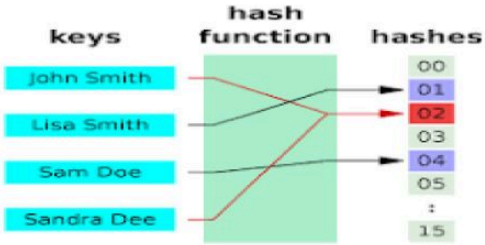
Digital Signature

- A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very high confidence that the message was created by a known sender (authenticity), and that the message was not altered in transit (integrity).
- Digital signatures are often used to implement electronic signatures, which includes any electronic data that carries the intent of a signature but not all electronic signatures use digital signatures

Scanned By Camera Scanner

Hash Function

- A hash function is any function that can be used to map data of arbitrary size to fixed-size values, though there are some hash functions that support variable length output. The values returned by a hash function are called hash values, hash codes, digests or simply hashes.



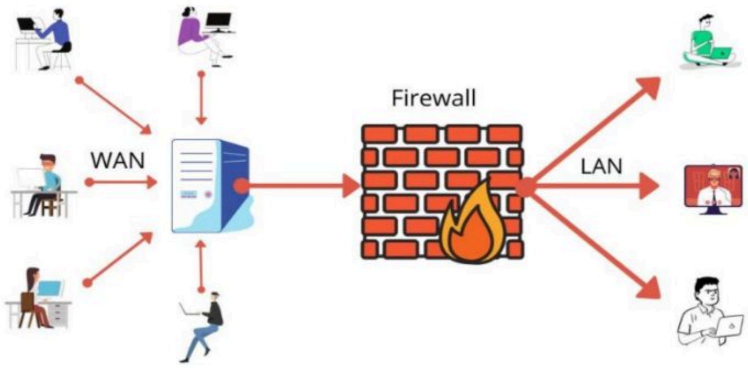
Scanned By Camera Scanner

Firewall

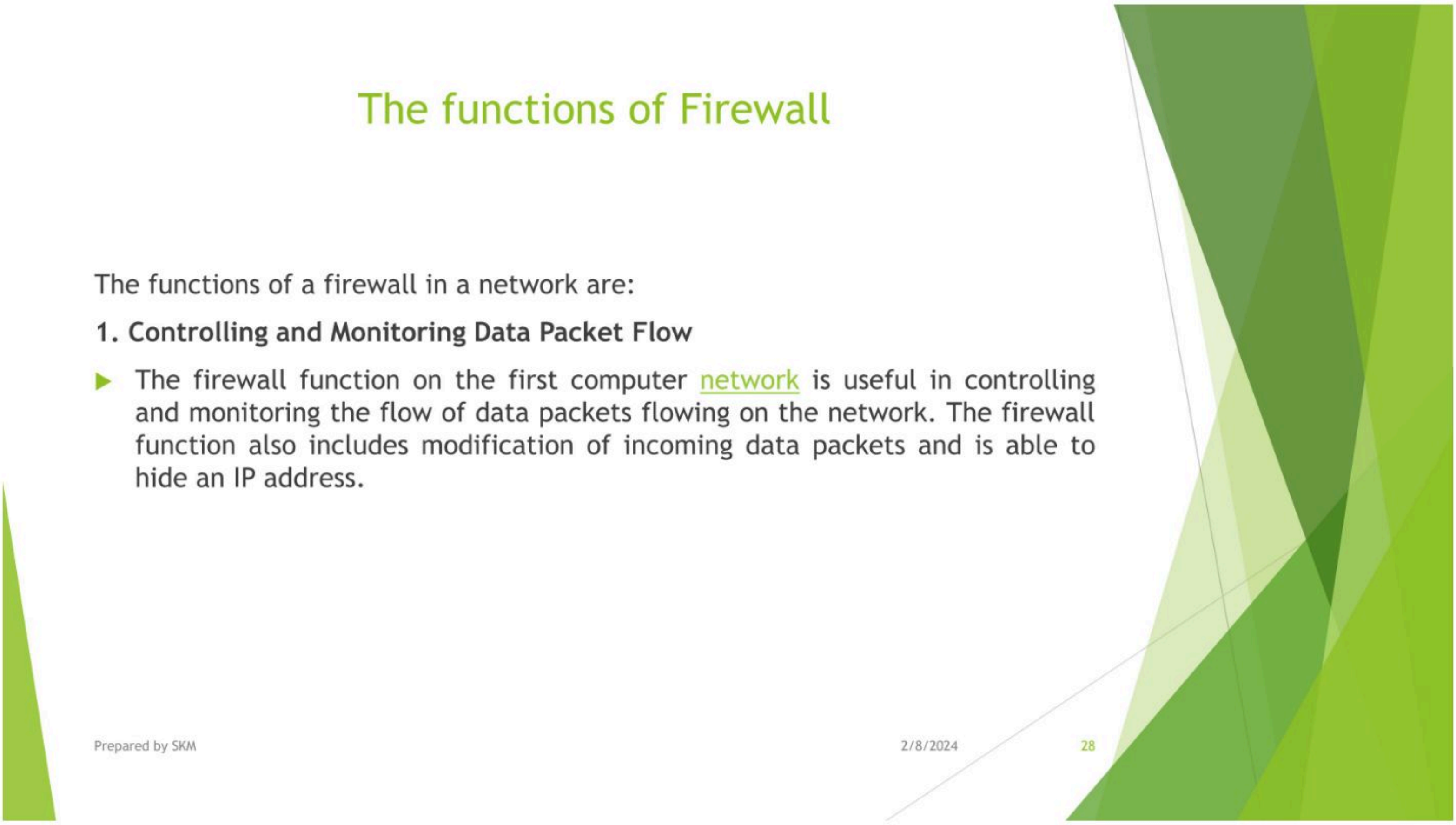
- A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

Scanned By Camera Scanner

Firewall



Scanned By Camera Scanner



The functions of Firewall

The functions of a firewall in a network are:

1. Controlling and Monitoring Data Packet Flow

- The firewall function on the first computer network is useful in controlling and monitoring the flow of data packets flowing on the network. The firewall function also includes modification of incoming data packets and is able to hide an IP address.

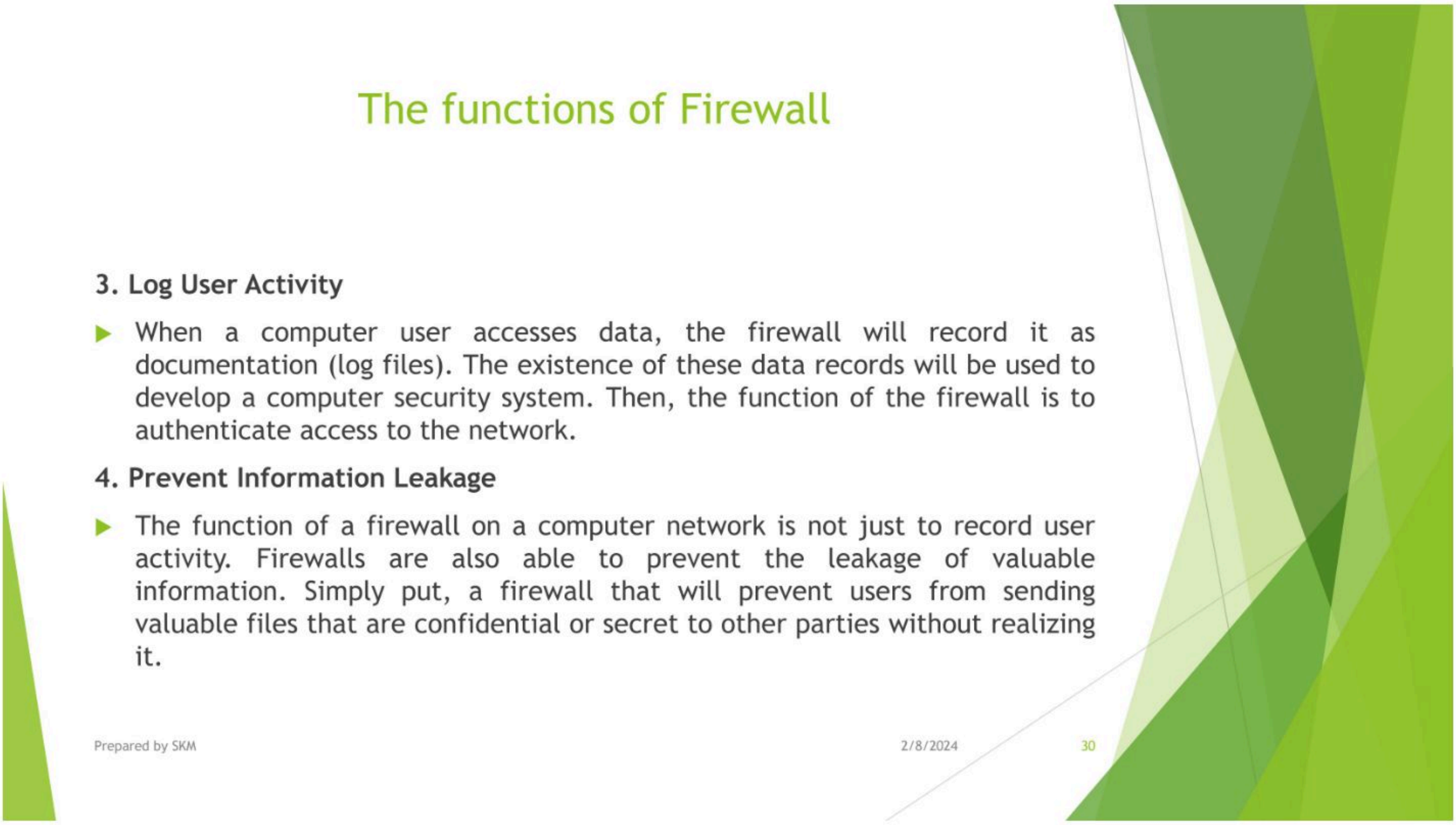
Scanned By Camera Scanner

The functions of Firewall

2. Become a Network Security Post

- The firewall function on a computer network is able to control data traffic when accessing a protected private network. All traffic either coming out or entering the network must pass through the firewall in order to be checked, either by filtering, limiting or even rejecting.

Scanned By Camera Scanner



The functions of Firewall

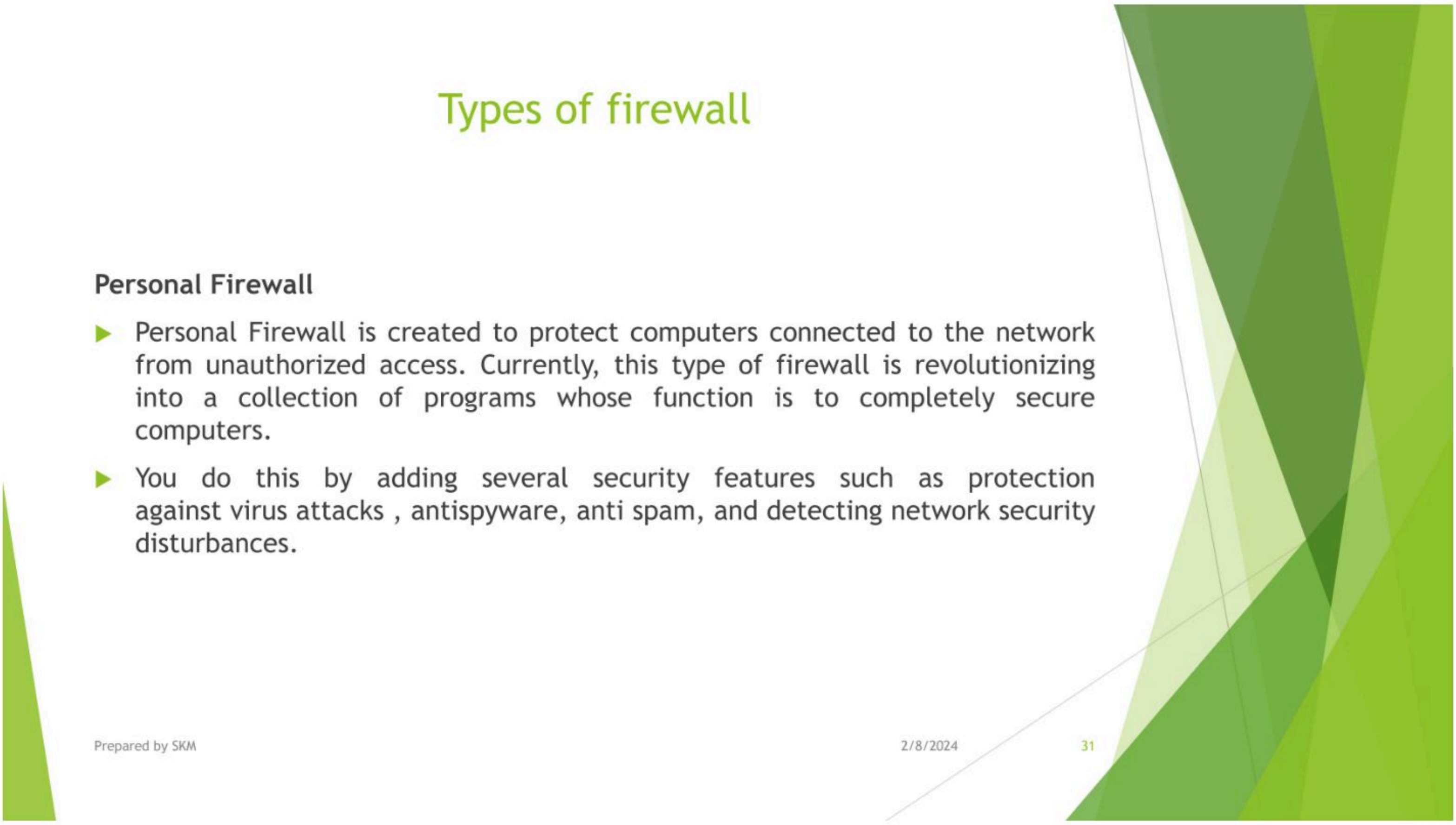
3. Log User Activity

- When a computer user accesses data, the firewall will record it as documentation (log files). The existence of these data records will be used to develop a computer security system. Then, the function of the firewall is to authenticate access to the network.

4. Prevent Information Leakage

- The function of a firewall on a computer network is not just to record user activity. Firewalls are also able to prevent the leakage of valuable information. Simply put, a firewall that will prevent users from sending valuable files that are confidential or secret to other parties without realizing it.

Scanned By Camera Scanner



Types of firewall

Personal Firewall

- Personal Firewall is created to protect computers connected to the network from unauthorized access. Currently, this type of firewall is revolutionizing into a collection of programs whose function is to completely secure computers.
- You do this by adding several security features such as protection against virus attacks , antispyware, anti spam, and detecting network security disturbances.

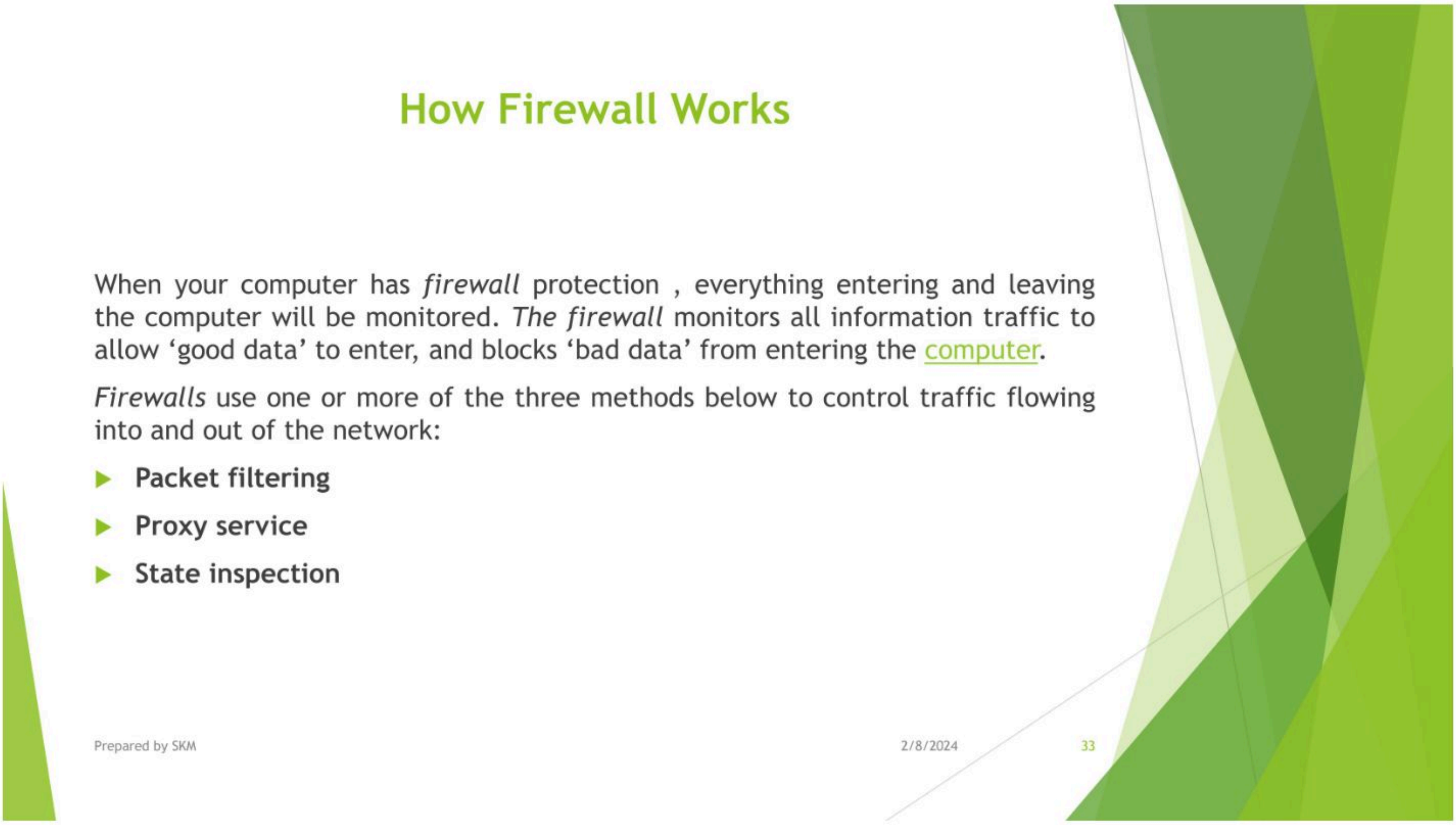
Scanned By Camera Scanner

Types of firewall

Network Firewall

- Overall network protection from all attacks is carried out by the Network Firewall. Network Firewall has several main features, namely Packet filter firewall and stateful firewall, Circuit Level Gateway, Application Level Gateway, and NAT Firewall. Network Firewalls are generally transparent to the user and use routing technology to determine which packets are allowed and which packets are rejected.

Scanned By Camera Scanner



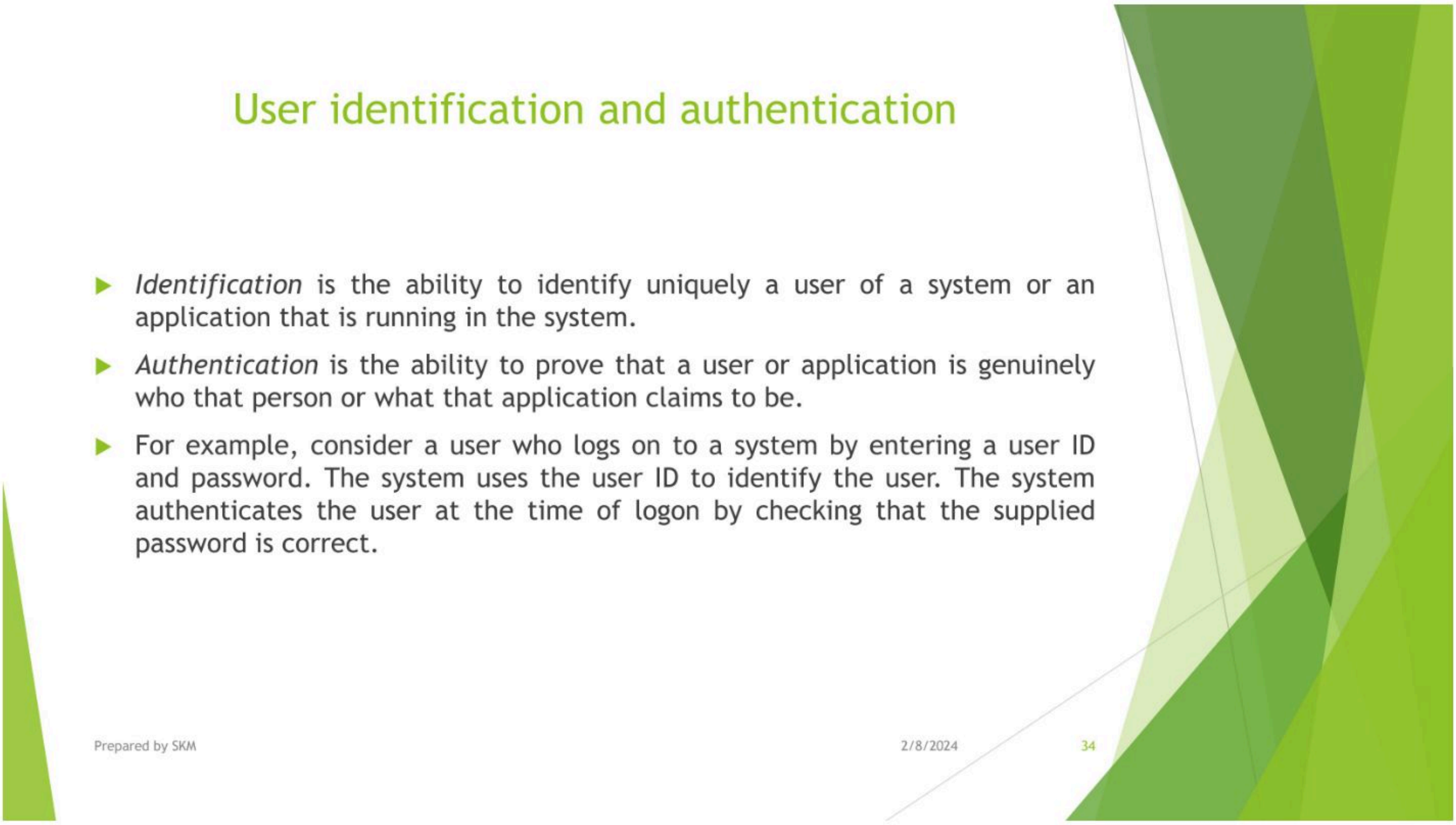
How Firewall Works

When your computer has *firewall* protection , everything entering and leaving the computer will be monitored. *The firewall* monitors all information traffic to allow ‘good data’ to enter, and blocks ‘bad data’ from entering the computer.

Firewalls use one or more of the three methods below to control traffic flowing into and out of the network:

- **Packet filtering**
- **Proxy service**
- **State inspection**

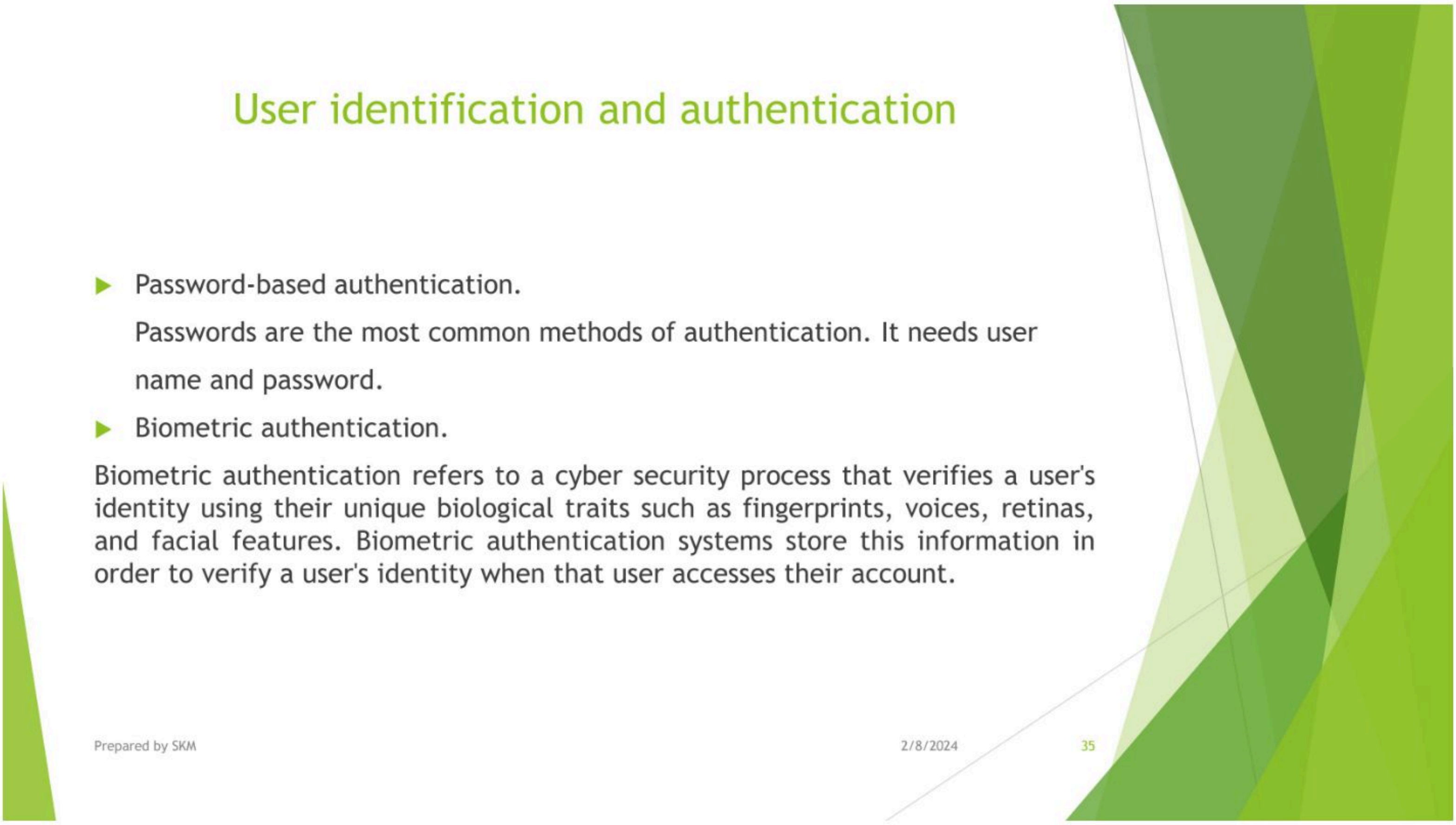
Scanned By Camera Scanner



User identification and authentication

- *Identification* is the ability to identify uniquely a user of a system or an application that is running in the system.
- *Authentication* is the ability to prove that a user or application is genuinely who that person or what that application claims to be.
- For example, consider a user who logs on to a system by entering a user ID and password. The system uses the user ID to identify the user. The system authenticates the user at the time of logon by checking that the supplied password is correct.

Scanned By Camera Scanner



User identification and authentication

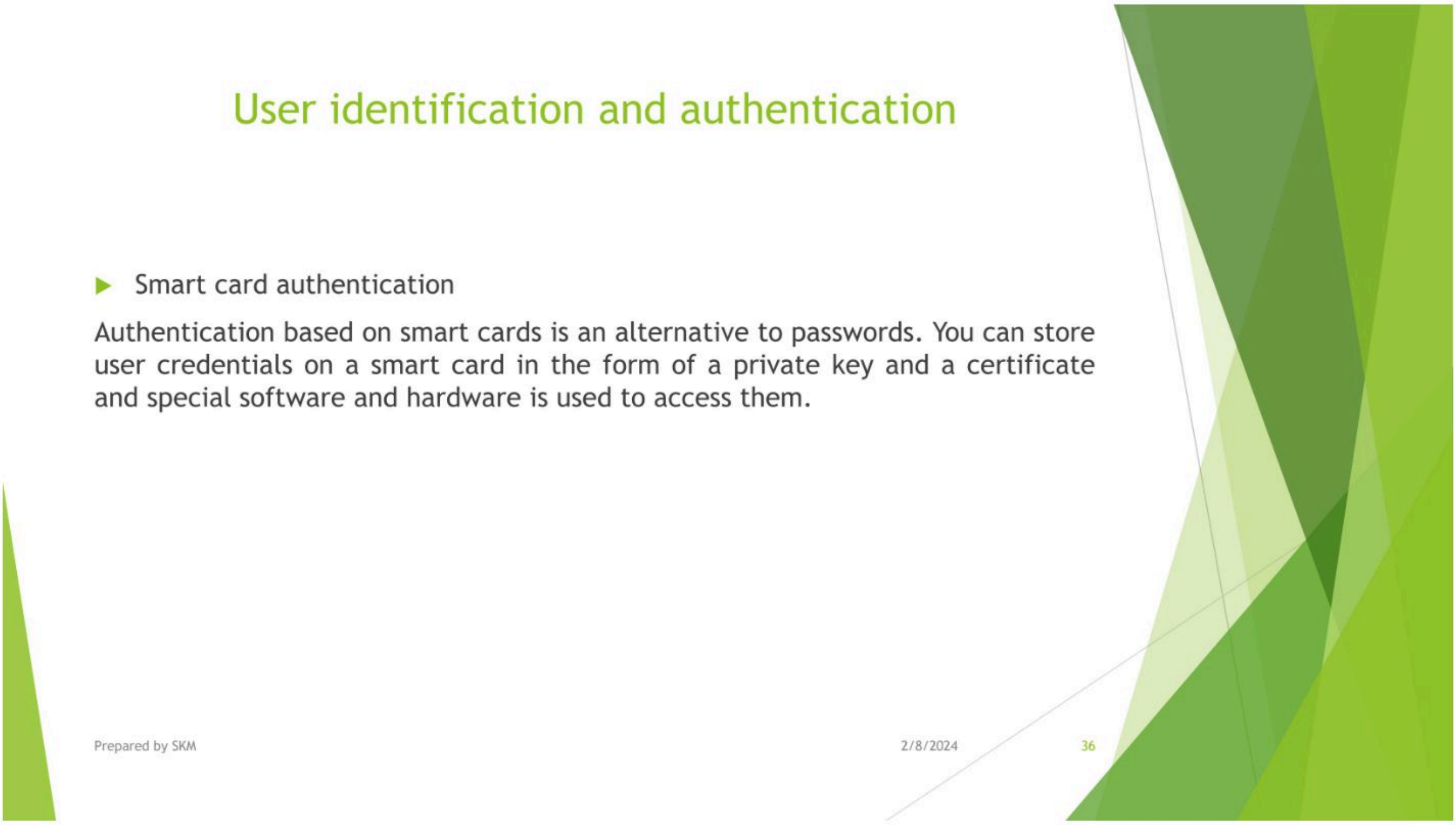
- Password-based authentication.

  Passwords are the most common methods of authentication. It needs user name and password.

- Biometric authentication.

Biometric authentication refers to a cyber security process that verifies a user's identity using their unique biological traits such as fingerprints, voices, retinas, and facial features. Biometric authentication systems store this information in order to verify a user's identity when that user accesses their account.

Scanned By Camera Scanner

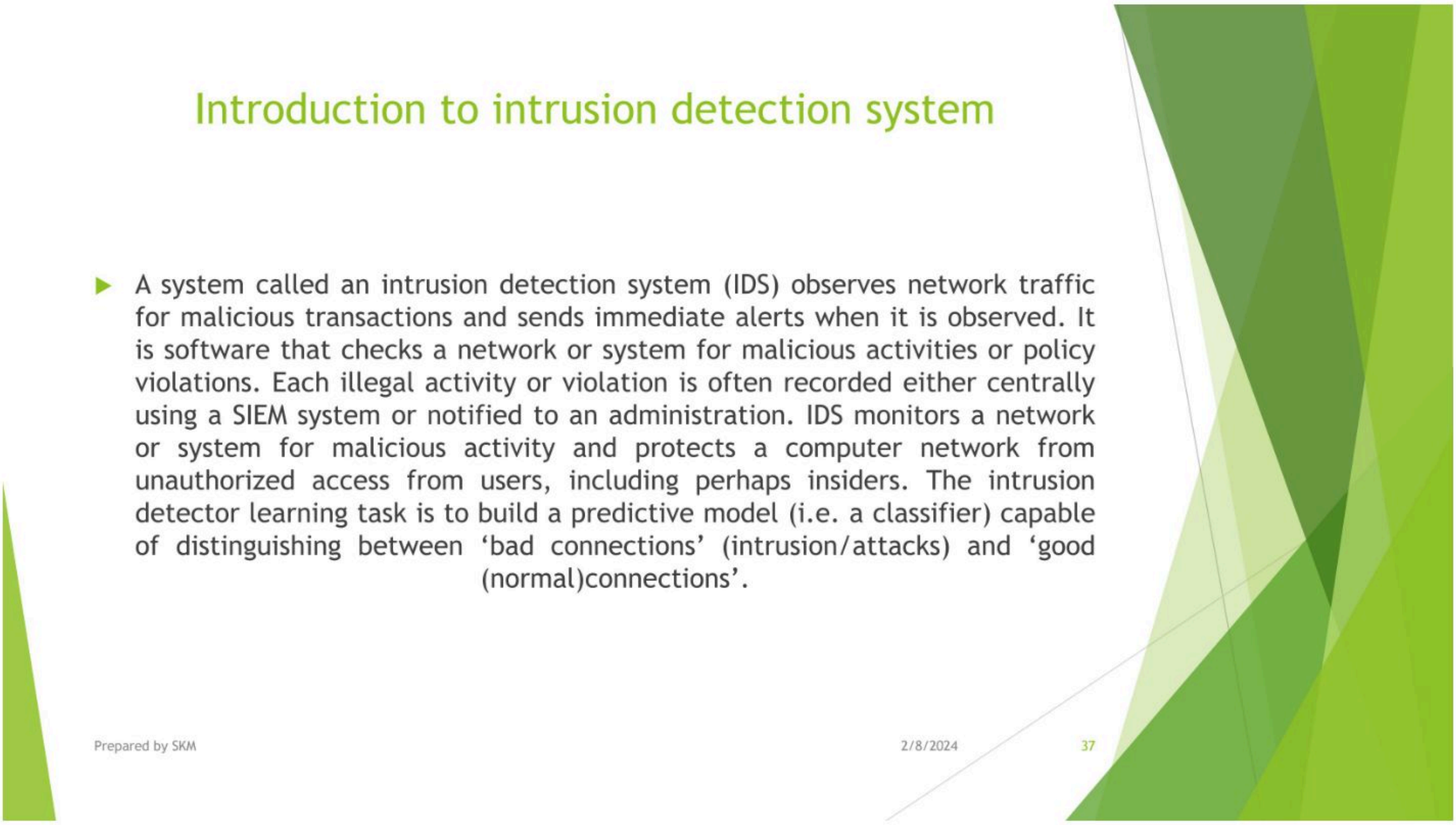


User identification and authentication

- Smart card authentication

Authentication based on smart cards is an alternative to passwords. You can store user credentials on a smart card in the form of a private key and a certificate and special software and hardware is used to access them.

Scanned By Camera Scanner

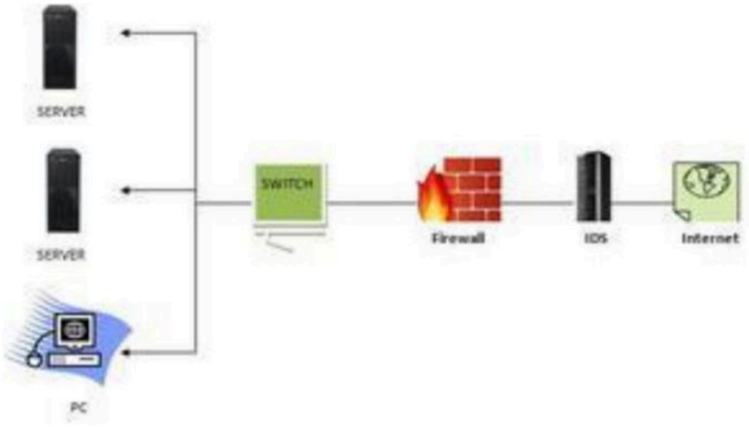


Introduction to intrusion detection system

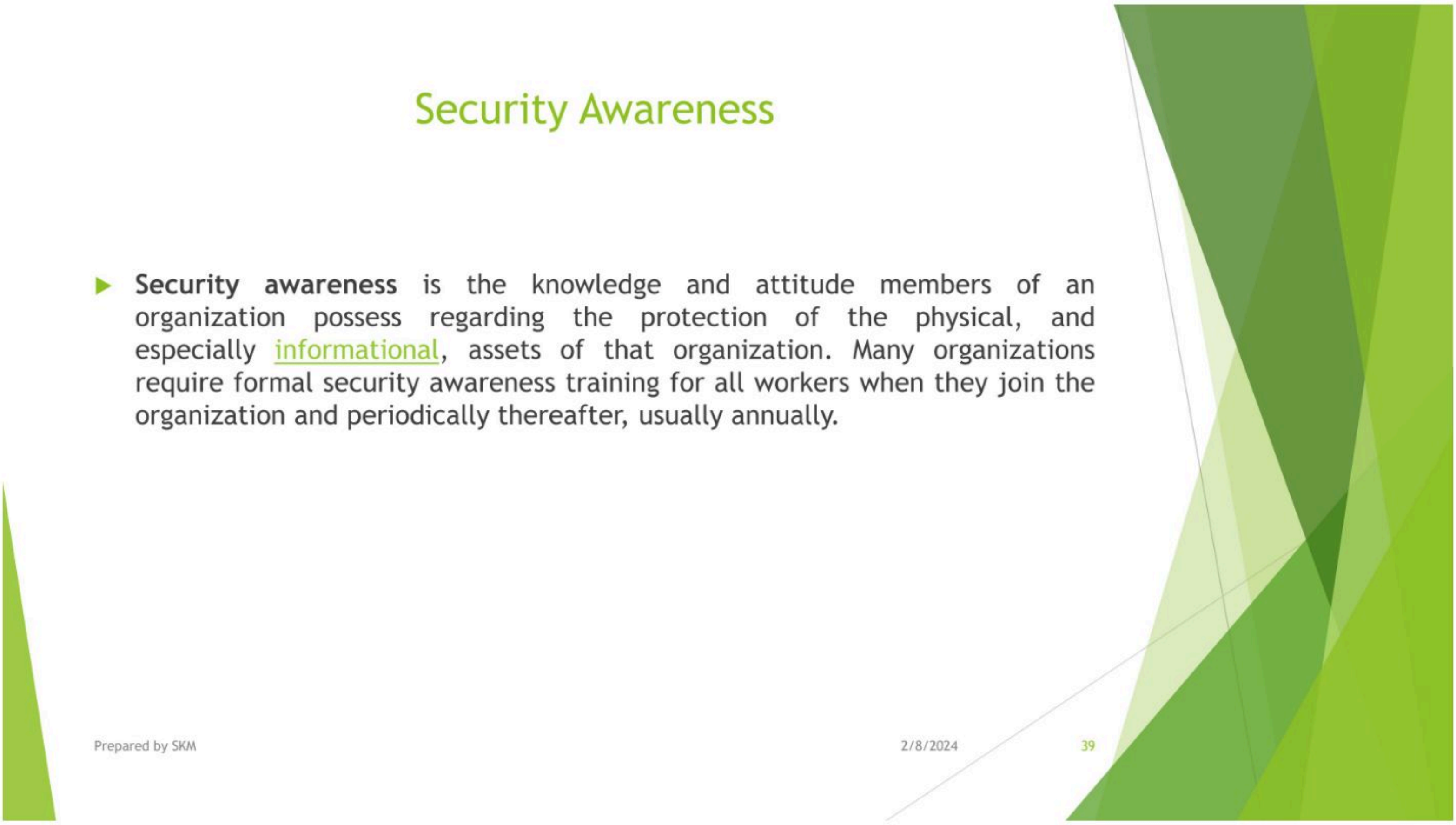
- A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations. Each illegal activity or violation is often recorded either centrally using a SIEM system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders. The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal)connections'.

Scanned By Camera Scanner

Introduction to intrusion detection system



Scanned By Camera Scanner



Security Awareness

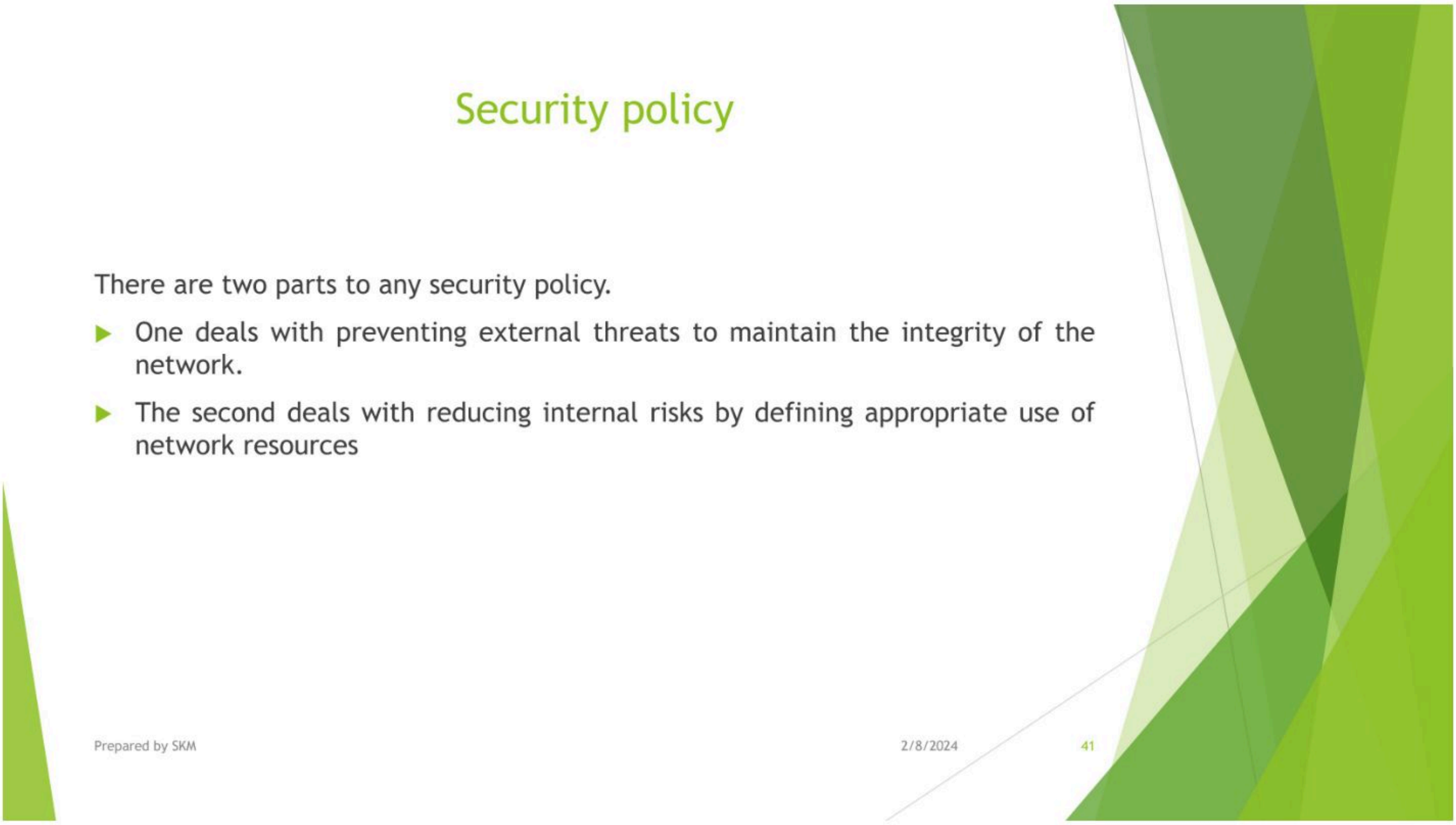
- **Security awareness** is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually.

Scanned By Camera Scanner

Security policy

- **Security policy** is a definition of what it means to *be secure* for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

Scanned By Camera Scanner



Security policy

There are two parts to any security policy.

- One deals with preventing external threats to maintain the integrity of the network.
- The second deals with reducing internal risks by defining appropriate use of network resources

Scanned By Camera Scanner

Seven elements of an effective security policy

- Clear purpose and objectives.
- Scope and applicability.
- Commitment from senior management.
- Realistic and enforceable policies.
- Clear definitions of important terms.
- Tailored to the organization's risk appetite.
- Up-to-date information.

Scanned By Camera Scanner

Effective guidelines for formulating security policy

- Identify your risks
- Learn from others
- Make sure the policy conforms to legal requirements
- Level of security = level of risk
- Include staff in policy development
- Train your employees
- Get it in writing
- Set clear penalties and enforce them
- Update your staff
- Install the tools you need

Scanned By Camera Scanner