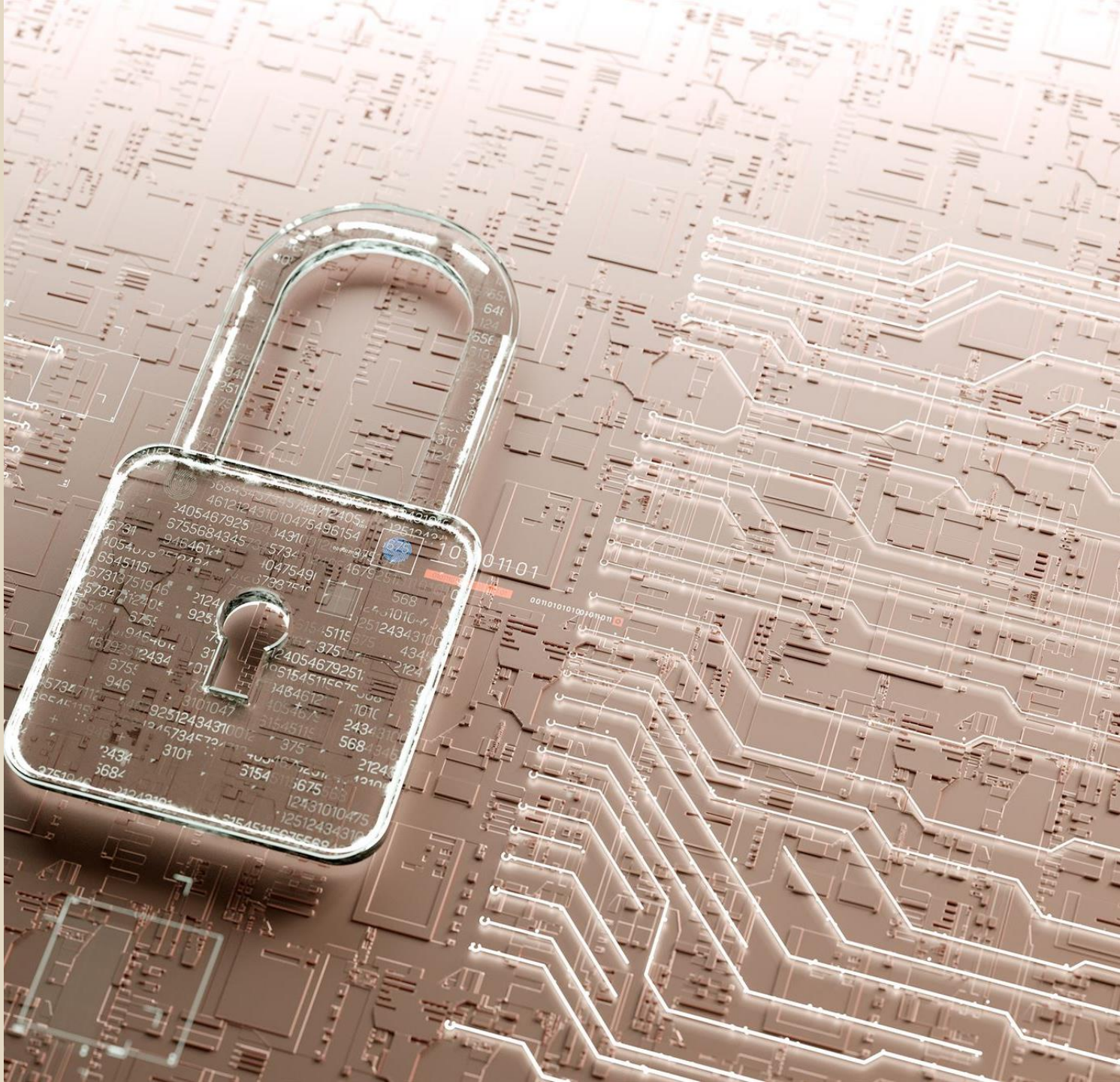
PROTECTING DATA AND INFORMATION

Ensuring security through effective data management



EXTERNAL THREATS TO DATA

VIRUSES AND MALWARE

Malware Definition and Impact

Viruses and malware can damage data, corrupt files, and disrupt computer performance significantly.

Common Infection Methods

Malware often spreads through email attachments, downloads, and infected websites, posing widespread risks.

Protection Strategies

Using antivirus software and regularly updating systems are essential defenses against malware threats.

ACCIDENTAL DAMAGE

Definition of Accidental Damage

Accidental damage means unintentional harm to IT systems or data caused by human error or mishaps.

Common Causes

Common causes include spilling liquids on devices and accidental deletion of important files.

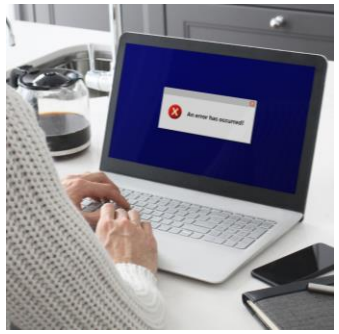
Consequences of Damage

Accidental damage can result in data loss or system failure, disrupting operations significantly.

Preventive Measures

Regular data backups and user training are essential to minimize the impact of accidental damage.

SOCIAL ENGINEERING



Manipulation Techniques

Social engineering uses tactics like phishing emails and deceptive calls to trick people into sharing sensitive information.

Human Vulnerability

These attacks exploit human error rather than weaknesses in technology or systems.

Prevention Strategies

Increasing awareness and education helps individuals recognize and prevent social engineering threats.

INTERNAL THREATS TO DATA

ACCESS TO INAPPROPRIATE WEBSITES

Risks of Unsafe Browsing

Accessing inappropriate websites can introduce malware and phishing threats to organizational IT systems.

Use of Web Filters

Implementing web filters helps control and restrict access to harmful or inappropriate websites effectively.

Staff Cybersecurity Training

Educating employees on safe browsing practices reduces security risks and promotes responsible internet use.

ACCIDENTAL DISCLOSURE OF DATA

Definition of Accidental Disclosure

Accidental disclosure happens when sensitive data is shared unintentionally, risking privacy and security breaches.

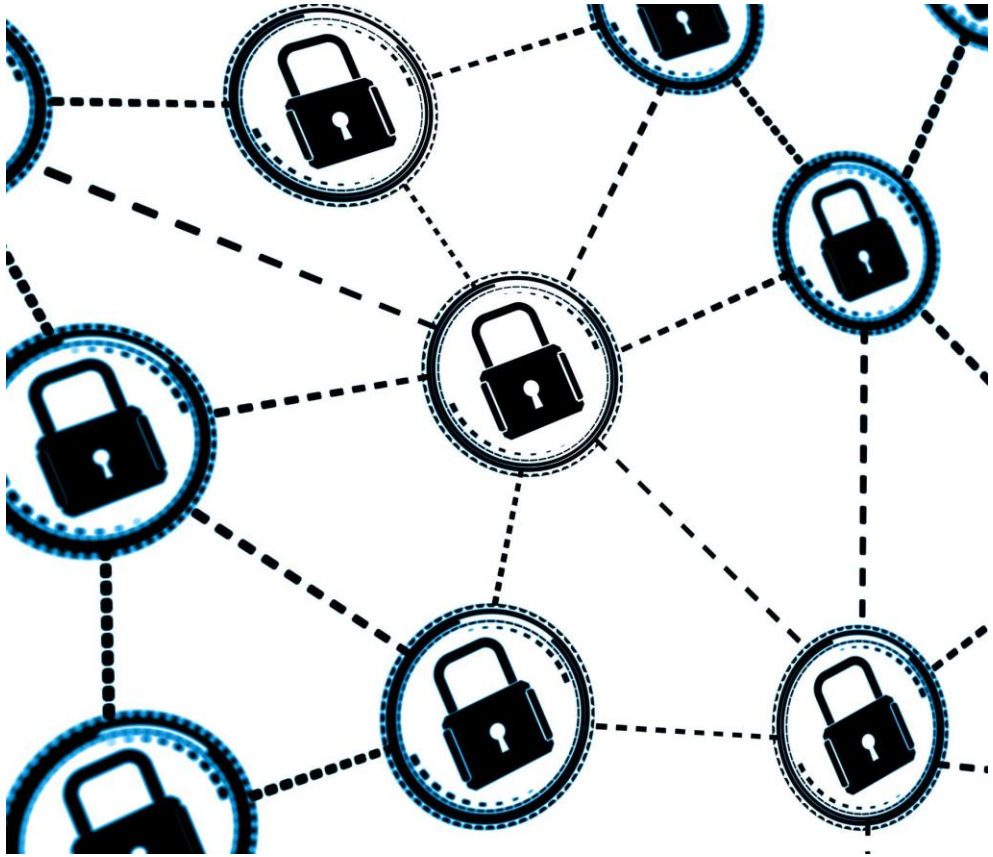
Consequences of Disclosure

Such disclosures can lead to serious privacy breaches and potential legal consequences for organizations.

Prevention Strategies

Training employees and using secure communication tools reduce the risk of accidental data disclosures.

STEALING OR LEAKING INFORMATION



Internal Threats

Internal staff can intentionally steal or leak sensitive information causing harm to the organisation.

Access Monitoring

Monitoring access to sensitive information helps detect and prevent unauthorized data breaches.

Encryption Usage

Encryption protects sensitive data by making it unreadable to unauthorized users.

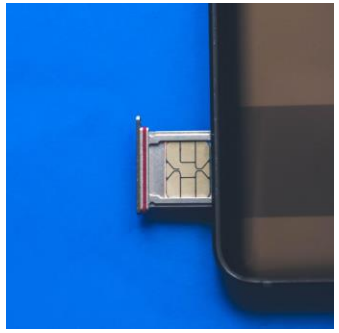
Strict Data Policies

Enforcing strict data policies ensures compliance and reduces the risk of internal data leaks.

USE OF PORTABLE DEVICES

Convenient Data Transfer

Portable devices enable easy and quick transfer of data between systems and users.



Security Risks

Lost or stolen portable devices can lead to exposure of sensitive information and data breaches.

Protection Measures

Organizations should use encryption and restrict device usage to safeguard sensitive data.

IMPACT OF DATA THREATS

LOSS OF DATA

Causes of Data Loss

Data loss can happen due to malware, accidental deletion, or hardware failure, affecting system operations.

Impact on Operations

Loss of important information disrupts business operations and can cause significant setbacks.

Prevention Methods

Regular backups and secure storage solutions are essential to prevent data loss effectively.

FINANCIAL LOSS DUE TO LEGAL ACTION

Legal Consequences of Data Breaches

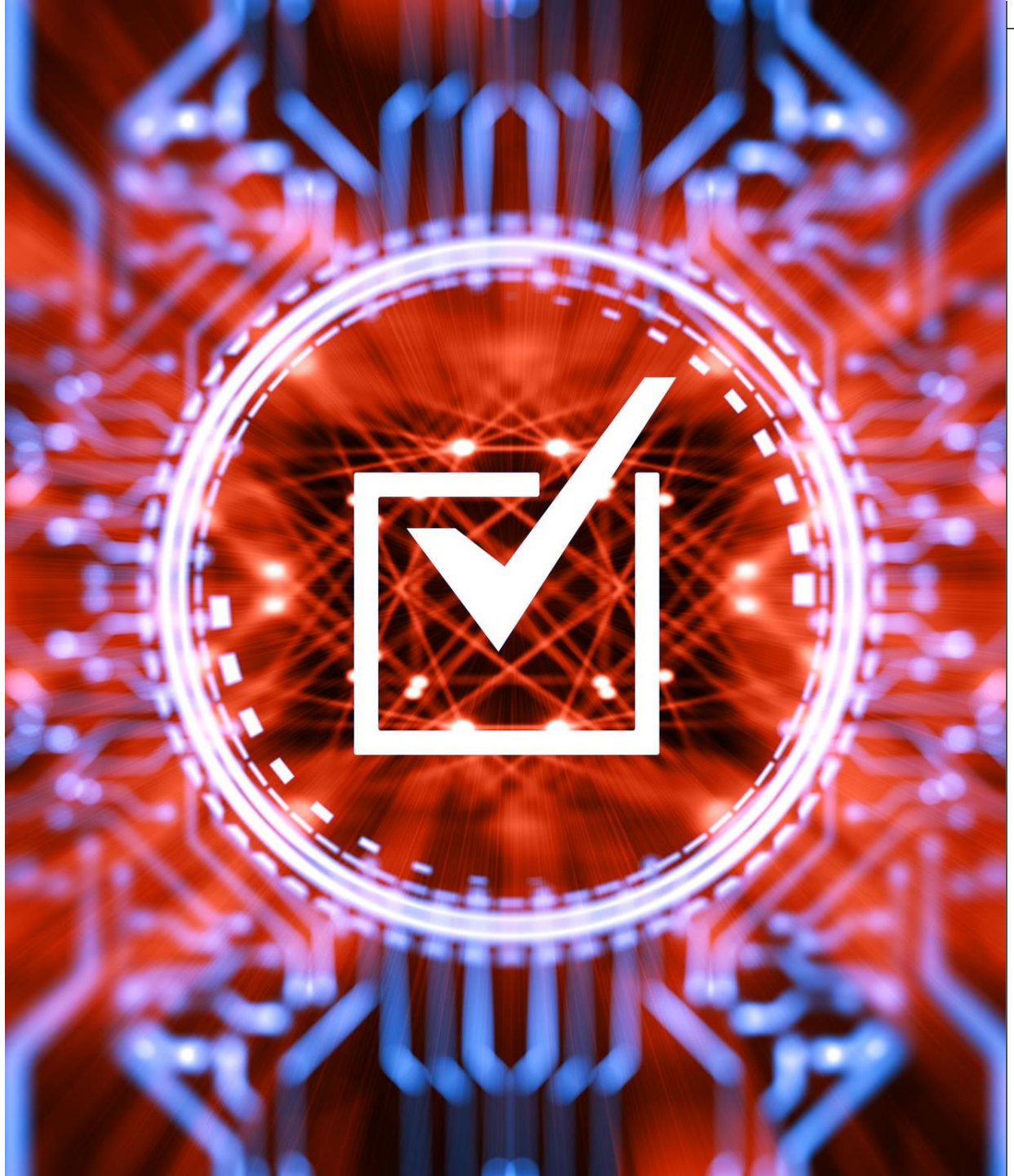
Data breaches can result in organisations facing legal actions such as lawsuits and regulatory penalties.

Financial Penalties and Fines

Fines imposed for violating data protection laws can lead to significant financial losses for organisations.

Importance of Regulatory Compliance

Ensuring compliance with data protection regulations helps organisations avoid costly legal and financial risks.



LOSS OF CUSTOMERS DUE TO PUBLIC IMAGE

Reputation Damage

Data breaches severely harm an organisation’s reputation, causing a loss of customer trust and credibility.

Negative Publicity Impact

Negative publicity from security incidents leads to reduced sales and long-term brand damage.

Maintaining Public Confidence

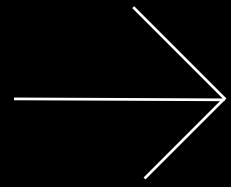
Transparent communication and robust security measures are critical to maintaining customer confidence.

Ensuring security and privacy in digital environments

RonsTechHub

Protecting Data in IT Systems

Techniques to Protect Data



File Permissions

Access Control Rules

File permissions define who can read, write, or execute a file, controlling user access effectively.

Data Protection

Permissions help protect sensitive data by limiting access to authorized users only.

Authorized Access

File permissions ensure only the right users can modify or view important file contents.

Access Levels

Defining User Permissions

Access levels specify which actions users can perform within a system, such as view, edit, or delete.

Controlling System Access

Access control helps organisations restrict actions to authorised users, reducing errors and misuse.

Backup and Recovery

Importance of Backup

Regular backups protect data from accidental deletion, hardware failure, and cyberattacks.

Recovery Procedures

Recovery tools help restore systems quickly to minimize downtime after data loss.

Passwords and Multi-Factor Authentication

Role of Passwords

Passwords serve as the primary defense mechanism protecting user accounts from unauthorized access.

Multi-Factor Authentication

Multi-factor authentication requires an additional verification step, increasing account security significantly.

Enhanced Security Benefits

Adding a second verification form makes it harder for attackers to access accounts even if passwords are compromised.

Biometrics

Physical Trait Verification

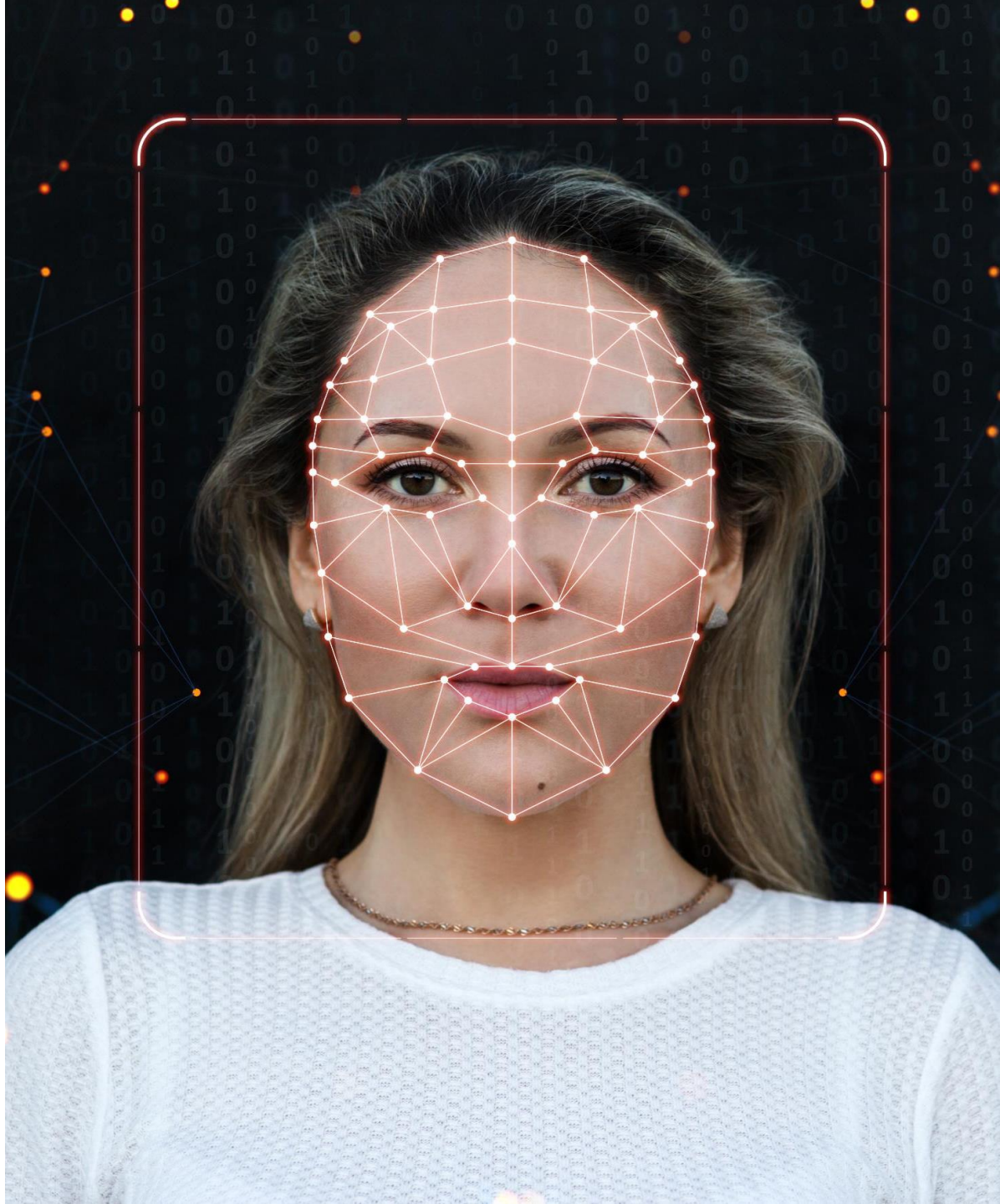
Biometrics use unique physical traits like fingerprints and facial features to verify identity accurately.

Enhanced Security

Biometric systems provide strong security by relying on unique individual characteristics that cannot be easily duplicated.

Common Applications

Biometrics are widely used in smartphones and secure buildings to prevent unauthorized access effectively.



Physical Access Control

Securing Physical Locations

Physical access control secures locations where sensitive data is stored to protect against unauthorized entry.

Use of Security Badges

Security badges grant authorized personnel access and help monitor entry into restricted areas.

Surveillance Monitoring

Surveillance cameras monitor physical spaces to deter and detect unauthorized access attempts.

Digital Certificates

Identity Verification

Digital certificates verify the identities of websites and users to establish trust in online environments.

Secure Data Transfer

Certificates ensure data is sent securely to the intended destination without interception by attackers.

Role in Online Security

Digital certificates are fundamental to secure online communication and protecting sensitive information.

Software Tools for Data Protection

Antivirus Software

Threat Detection

Antivirus software scans computers to identify harmful programs like viruses and malware effectively.

Threat Removal

The software removes detected threats to prevent damage to data and system integrity.

Regular Updates

Frequent software updates ensure protection against new and evolving cyber threats.

Firewalls

Network Barrier Function

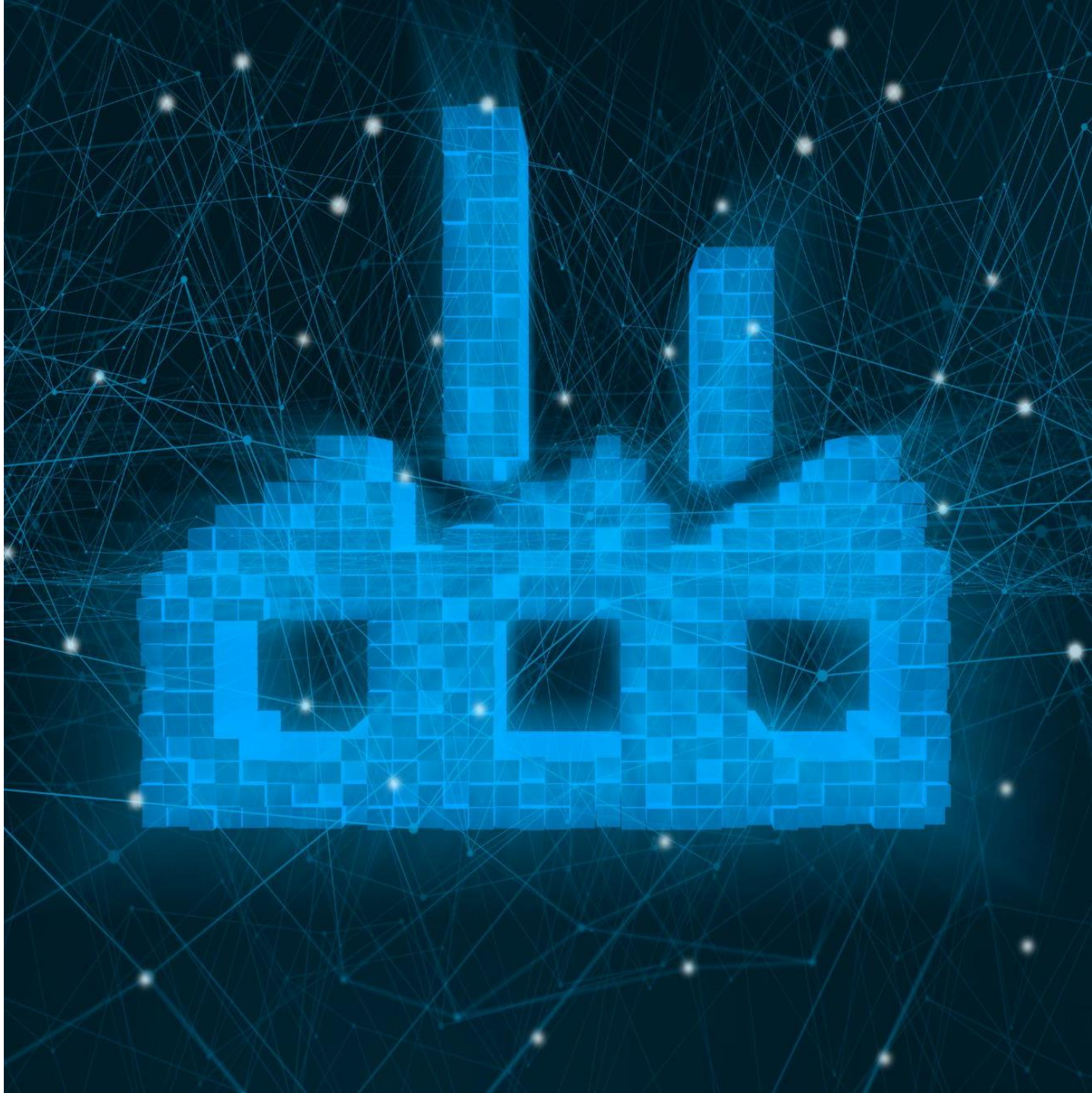
Firewalls act as barriers between trusted and untrusted networks to enforce security policies.

Traffic Monitoring

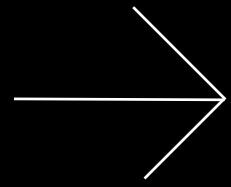
Firewalls monitor incoming and outgoing data traffic to detect and block harmful information.

Preventing Unauthorized Access

Firewalls prevent unauthorized access and protect systems from cyber threats effectively.



Encryption Methods



Encrypting Stored Data

Purpose of Encryption

Encryption transforms data into a coded format to protect it from unauthorized access.

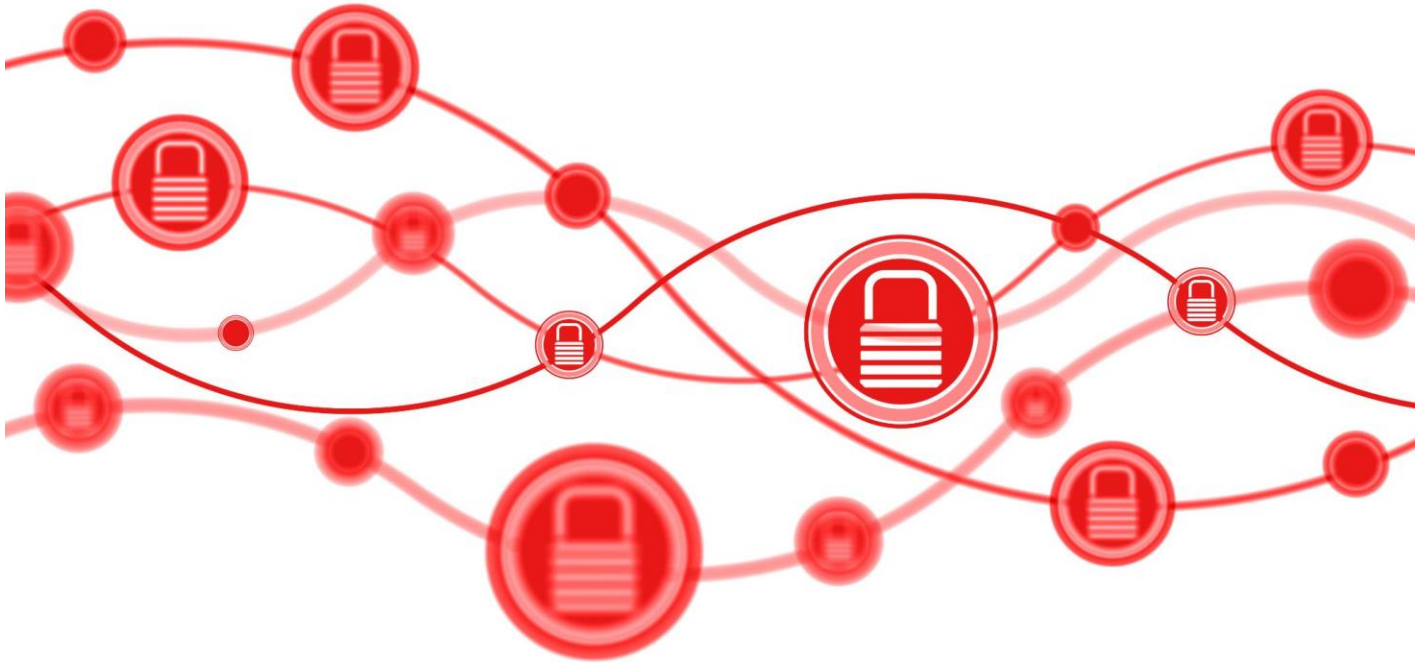
Protection of Stored Files

Encrypting stored files ensures data remains unreadable without the correct decryption key.

Importance for Sensitive Data

Encryption is vital to safeguard sensitive information against theft or unauthorized use.

Encrypting Data During Transmission



Data Interception Risks

Information sent over the internet is vulnerable to interception by unauthorized parties.

Importance of Encryption

Encryption secures data during transmission, preventing unauthorized access and ensuring privacy.

Critical Applications

Encryption is essential for securing emails, online payments, and file transfers.

HTTPS for Secure Websites

What is HTTPS

HTTPS is the secure version of HTTP that encrypts data between websites and users.

Data Encryption Benefits

Encryption protects sensitive information such as passwords and credit cards from theft.