

# Cybersecurity Procedures, Techniques, and Technologies

Cybersecurity involves various procedures, techniques, and technologies to safeguard systems, networks, and data from cyber threats. Below is an in-depth look at these aspects with examples.

## Procedures

### Incident Response Plan (IRP):

A structured process to handle security incidents effectively. Example: During a ransomware attack, a company follows its IRP to isolate infected systems, notify stakeholders, and recover backups.

### Security Audits:

Regular assessments of security policies and systems. Example: A company conducts a quarterly audit to ensure compliance with GDPR standards.

### Patch Management:

Updating software to address vulnerabilities. Example: Applying a security patch to fix a zero-day vulnerability in Windows OS.

### Backup and Recovery:

Creating regular backups and having recovery plans. Example: Using cloud backups to restore critical files after a cyberattack.

## Techniques

### Firewall Implementation:

Filters network traffic based on security rules. Example: A company uses a Web Application Firewall (WAF) to block SQL injection attacks.

### Encryption:

Secures data using cryptographic algorithms. Example: Encrypting emails with PGP to ensure confidentiality.

### **Penetration Testing:**

Simulating attacks to identify vulnerabilities. Example: Ethical hackers test a banking app for flaws before deployment.

## **Technologies**

### **Antivirus Software:**

Detects and removes malicious software. Example: Using Norton Antivirus to block and quarantine malware.

### **Virtual Private Network (VPN):**

Encrypts internet traffic to protect privacy. Example: A remote worker uses a VPN to access company systems securely.

### **Security Information and Event Management (SIEM):**

Analyzes security data in real-time. Example: Splunk SIEM detects an unusual login attempt from an unknown location.