

Sample Questions with Answers

Cybersecurity - Ethical Hacking

Generated on June 13, 2026 at 11:34 AM

Cybersecurity

[NOTE] Important Note: This PDF contains sample questions with complete answers and explanations. Visit [SolveMyQues.com](https://www.solvemyques.com) for our complete question bank, interactive tests, and detailed performance tracking!

Question 1:

What is cybersecurity and why is it important?

[ANSWER] Answer & Explanation:

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage.

What cybersecurity protects:

- Confidentiality** - Ensuring data is only accessible to authorized users
- Integrity** - Maintaining accuracy and completeness of data
- Availability** - Ensuring systems and data are accessible when needed

Why cybersecurity is critical:

- Financial protection** - Prevents costly data breaches and ransomware
- Privacy protection** - Safeguards personal and sensitive information
- Business continuity** - Maintains operations and prevents downtime
- Regulatory compliance** - Meets legal requirements (GDPR, HIPAA, SOX)
- Reputation management** - Protects brand trust and customer confidence

Common threats addressed:

- Malware (viruses, ransomware, trojans)
- Phishing and social engineering attacks
- Data breaches and identity theft
- Denial of Service (DoS) attacks
- Insider threats and human error

Real-world impact:

Cyberattacks cost businesses an average of \$4.45 million per breach (2023). Major incidents like Equifax (147M records), Target (40M+ cards), and Colonial Pipeline (infrastructure shutdown) demonstrate the devastating consequences of inadequate cybersecurity.

Best practices:

- Implement defense-in-depth strategy
- Regular security awareness training
- Keep systems updated and patched
- Use strong authentication methods
- Monitor and respond to threats continuously

Question 2:

What are the different types of malware and how do they work?

[ANSWER] Answer & Explanation:

Malware (malicious software) is designed to damage, disrupt, or gain unauthorized access to computer systems.

Major malware types:

- 1. Viruses:** How they work - Attach to legitimate files and replicate when executed
Spread method - Through infected files, email attachments, removable media
Example - ILOVEYOU virus (2000) infected 50M+ computers via email
- 2. Worms:** How they work - Self-replicating programs that spread across networks
Spread method - Exploit network vulnerabilities without user interaction
Example - WannaCry ransomware worm (2017) affected 300k+ computers
- 3. Trojans:** How they work - Disguise as legitimate software to trick users
Purpose - Create backdoors, steal data, or download additional malware
Example - Banking trojans that steal financial credentials
- 4. Ransomware:** How they work - Encrypt files and demand payment for decryption key
Impact - Can paralyze entire organizations and critical infrastructure
Example - Colonial Pipeline attack (2021) disrupted US fuel supply
- 5. Spyware:** How they work - Secretly monitor and collect user information
Data stolen - Passwords, browsing habits, personal information
Example - Keyloggers that record keystrokes
- 6. Adware:** How they work - Display unwanted advertisements and track behavior
Impact - Slows system performance and compromises privacy

Protection strategies:

- Use reputable antivirus software
- Keep systems and software updated
- Avoid suspicious downloads and email attachments
- Regular system backups
- Network segmentation and access controls



Question 3:

What is the difference between authentication and authorization?

[ANSWER] Answer & Explanation:

Authentication and authorization are fundamental security concepts that work together to control system access.

Authentication - "Who are you?"
Purpose - Verifies the identity of a user or system
Process - User provides credentials to prove their identity
Methods - Username/password, biometrics, smart cards, tokens
Example - Entering your username and password to log into email

Authorization - "What can you do?"
Purpose - Determines what resources an authenticated user can access
Process - System checks user permissions against requested resources
Methods - Role-based access control (RBAC), access control lists (ACLs)
Example - Admin can delete files, regular user can only read them

Key differences:

Aspect	Authentication	Authorization
Question	Who are you?	What can you access?
When	First step	After authentication
Verifies	Identity	Permissions
Methods	Passwords, biometrics	Roles, policies
Failure	Access denied	Limited access

Real-world example:

- 1. Authentication** - Employee badges into office building (proves identity)
- 2. Authorization** - Badge allows access to specific floors/rooms (defines permissions)

Multi-factor authentication (MFA): Combines multiple authentication factors:

- **Something you know** - Password, PIN
- **Something you have** - Phone, token, smart card
- **Something you are** - Fingerprint, face recognition

Best practices:

- Implement strong authentication (MFA)
- Follow principle of least privilege
- Regular access reviews and updates
- Separate admin and user accounts
- Monitor and log access attempts

Question 4:

What is a firewall and how does it protect networks?

[ANSWER] Answer & Explanation:

A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

How firewalls work:

- Traffic filtering** - Examines data packets and applies security rules
- Access control** - Allows or blocks traffic based on source, destination, port
- Network barrier** - Creates a protective boundary between trusted and untrusted networks
- Logging** - Records traffic patterns and security events for analysis

Types of firewalls:

- Packet filtering (Stateless):**
 - Function** - Examines individual packets against static rules
 - Criteria** - Source/destination IP, port numbers, protocol type
 - Pros** - Fast processing, low resource usage
 - Cons** - Cannot track connection state, limited security
- Stateful inspection:**
 - Function** - Tracks connection state and context
 - Intelligence** - Remembers previous packets in the connection
 - Security** - Better protection against sophisticated attacks
 - Example** - Allows return traffic for established connections
- Application layer (Proxy):**
 - Function** - Inspects application-specific data and protocols
 - Deep inspection** - Understands HTTP, FTP, SMTP content
 - Security** - Highest level of protection and control
 - Performance** - Slower due to detailed analysis
- Next-generation firewalls (NGFW):**
 - Features** - Combines traditional firewall with IPS, application awareness
 - Intelligence** - User identity, application control, threat intelligence
 - Integration** - Works with security information and event management (SIEM)

Firewall deployment:

- Network perimeter** - Between internal network and internet
- Internal segmentation** - Between network zones (DMZ, servers, workstations)
- Host-based** - Software firewall on individual devices

Best practices:

- Default deny policy (block all, allow specific)
- Regular rule review and cleanup
- Monitor firewall logs for threats
- Keep firmware updated
- Test firewall rules and configurations

Question 5:

What is phishing and how can organizations protect against it?

[ANSWER] Answer & Explanation:

Phishing is a social engineering attack where cybercriminals impersonate legitimate entities to steal sensitive information like passwords, credit card numbers, or personal data.

How phishing works:

- Deception** - Attackers create fake emails, websites, or messages
- Urgency** - Create false sense of urgency to bypass critical thinking
- Credential harvesting** - Trick users into entering sensitive information
- Malware delivery** - Distribute malicious attachments or links

Common phishing types:

- Email phishing:**
 - Method** - Mass emails impersonating banks, services, or colleagues
 - Example** - "Your account will be suspended, click here to verify"
 - Indicators** - Generic greetings, urgent language, suspicious links
- Spear phishing:**
 - Method** - Targeted attacks using personal information
 - Research** - Attackers study victims through social media, company websites
 - Example** - CEO impersonation requesting urgent wire transfer
- Whaling:**
 - Target** - High-profile executives and decision makers
 - Impact** - Access to sensitive corporate information and systems
 - Sophistication** - Highly personalized and convincing attacks
- Smishing (SMS phishing):**
 - Method** - Text messages with malicious links or requests
 - Example** - "Package delivery failed, click to reschedule"
- Vishing (Voice phishing):**
 - Method** - Phone calls impersonating legitimate organizations
 - Example** - Fake tech support requesting remote access

Protection strategies:

- Technical controls:**
 - Email security gateways with anti-phishing filters
 - Web filtering to block malicious websites
 - Multi-factor authentication (MFA)
 - Email authentication (SPF, DKIM, DMARC)
- User education:**
 - Regular security awareness training
 - Simulated phishing exercises
 - Clear reporting procedures for suspicious emails
 - Verification protocols for sensitive requests

Best practices:

- Verify sender identity through separate communication channel
- Hover over links to check actual destination
- Be suspicious of urgent or threatening language
- Never provide sensitive information via email or phone
- Keep software and browsers updated

[FEATURES] Want More Questions & Features?

Visit [SolveMyQues.com](https://www.solvemyques.com) for:

- [+] Complete question bank with detailed answers & explanations
- [+] Interactive skill assessment tests with instant results
- [+] Performance tracking and personalized recommendations
- [+] Achievement certificates and progress reports
- [+] Expert explanations and step-by-step solutions
- [+] Ask questions to our expert team
- [+] Daily challenges and leaderboards

[WEB] Website: www.solvemyques.com

[EMAIL] Email: support@solvemyques.com

SolveMyQues