Cyber Security Cheat Sheet

1. CIA Triad (Core Principles)
- Confidentiality: Prevent unauthorized access (e.g., encryption).
- Integrity: Ensure data accuracy and consistency (e.g., hashing, checksums).
- Availability: Ensure resources are accessible (e.g., backups, DDoS protection).

2. Common Threats
- Phishing: Fake emails/websites to steal data.
- Malware: Malicious software (virus, worm, trojan).
- Ransomware: Encrypts files, demands ransom.
- SQL Injection: Insert malicious SQL in web input.
- XSS (Cross-Site Scripting): Injects script into websites.
- Man-in-the-Middle (MitM): Intercepts communication.
- Brute Force Attack: Tries all combinations to crack passwords.

3. Authentication & Authorization
- Authentication: Who are you? (e.g., passwords, biometrics).
- Authorization: What can you access? (e.g., permissions, roles).

4. Security Tools
- Wireshark: Network traffic analysis.
- Nmap: Port scanning/network mapping.
- Metasploit: Exploit vulnerabilities.
- Burp Suite: Web vulnerability testing.
- John the Ripper: Password cracking.

5. Best Practices
- Use strong passwords (12+ chars, symbols, mix-case).
- Enable 2FA (Two-Factor Authentication).
- Regularly update software & patches.
- Don't click suspicious links or attachments.
- Use VPN on public Wi-Fi.
- Backup data regularly (offline & cloud).
- Employ firewalls & antivirus software.

6. Key Concepts
- Firewall: Blocks unauthorized access.

Cyber Security Cheat Sheet

- IDS/IPS: Detects/Prevents intrusions.
- Encryption: Converts data to unreadable form.
- Hashing: One-way data transformation (e.g., SHA-256).
- Social Engineering: Manipulating people to reveal info.

7. Important Acronyms
- VPN: Virtual Private Network
- DDoS: Distributed Denial of Service
- HTTPS: HTTP + SSL/TLS (secure)
- SSL/TLS: Secure Sockets Layer / Transport Layer Security
- IAM: Identity & Access Management