

CYBER SECURITY FUNDAMENTALS

TechRacine Academy

https://techracine.com

https://academy.techracine.com

Table of Contents

1. Introduction to Cyber Security 3
2. Why Cyber Security Matters 3
3. Understanding the CIA Triad 3
4. Common Cyber Threats 4
5. Malware and Ransomware 4
6. Phishing and Social Engineering 4
7. Password Security and Authentication 4
8. Multi-Factor Authentication 5
9. Network Security 5
10. Firewalls and Secure Communication 5
11. Data Security and Encryption 6
12. Web Application Security 6
13. API Security 6
14. Endpoint Security 7
15. Cloud Security 7
16. Identity and Access Management 7
17. Secure Software Development 7
18. Security Monitoring and Incident Detection 8
19. Incident Response and Recovery 8
20. Cyber Security Best Practices 8
21. Common Cyber Security Mistakes 9
22. Cyber Security in Real World Applications 9
23. Summary 10
24. Exercises 10

1. Introduction to Cyber Security

Cyber security is the practice of protecting computers, networks, applications, systems, and data from unauthorized access, misuse, damage, or disruption.

Modern organizations depend on digital systems, so security is an important part of software and information technology.

Cyber security includes technical controls, secure development practices, user awareness, monitoring, and response procedures.

A strong security approach aims to protect information while allowing authorized users to use systems effectively.

2. Why Cyber Security Matters

Cyber security helps protect confidential information, business systems, customer data, and digital services.

Security incidents can cause financial loss, service disruption, data exposure, and damage to an organization's reputation.

Security is not only the responsibility of a security team; developers, administrators, employees, and users all contribute to safer systems.

Security should be considered during system design and development rather than added only after deployment.

3. Understanding the CIA Triad

The CIA triad is a basic security model based on Confidentiality, Integrity, and Availability.

Confidentiality means information should be accessible only to authorized people or systems.

Integrity means information should remain accurate and should not be changed without authorization.

Availability means authorized users should be able to access systems and information when needed.

4. Common Cyber Threats

Cyber threats are actions or events that can compromise the confidentiality, integrity, or availability of systems.

Common threats include phishing, malware, password attacks, unauthorized access, denial-of-service attacks, and data theft.

Threats can target people, applications, networks, devices, cloud services, or organizational processes.

Understanding common threats helps teams select suitable preventive and detective controls.

5. Malware and Ransomware

Malware is malicious software designed to perform unauthorized or harmful actions.

Examples include viruses, worms, trojans, spyware, and ransomware.

Ransomware can make files or systems unavailable and may demand payment from victims.

Regular updates, secure backups, endpoint protection, access controls, and user awareness can reduce malware-related risk.

6. Phishing and Social Engineering

Phishing uses deceptive messages or websites to trick users into revealing information or performing unsafe actions.

Social engineering focuses on manipulating people rather than only attacking technical systems.

Attackers may use email, messages, phone calls, or fake login pages to appear trustworthy.

Users should verify unexpected requests, avoid suspicious links and attachments, and report suspected phishing attempts.

7. Password Security and Authentication

Authentication verifies the identity of a user or system.

Strong passwords should be difficult to guess and should not be reused across important accounts.

Password managers can help users create and store unique passwords.

Systems should protect stored credentials and should avoid exposing passwords in logs, source code, or error messages.

8. Multi-Factor Authentication

Multi-factor authentication (MFA) requires more than one type of authentication factor.

Common factors include something the user knows, something the user has, and something the user is.

MFA provides additional protection when a password is stolen or guessed.

Organizations should enable MFA for important accounts and administrative access whenever appropriate.

9. Network Security

Network security protects communication systems and network resources from unauthorized access and attacks.

Controls may include network segmentation, secure protocols, firewalls, access controls, monitoring, and intrusion detection.

Segmenting networks can limit the movement of an attacker if one system is compromised.

Network traffic should be monitored for unusual behavior and unauthorized connections.

10. Firewalls and Secure Communication

Firewalls control network traffic according to defined security rules.

They can help restrict unwanted connections between networks, devices, and services.

Secure communication protocols help protect information while it travels between systems.

Security rules should be reviewed regularly so that unnecessary access is removed.

11. Data Security and Encryption

Data security protects information during storage, processing, and transmission.

Encryption transforms readable information into a protected form that requires the appropriate key or mechanism to access.

Encryption can be used for data in transit and data at rest.

Access control, backups, data classification, and secure key management should complement encryption.

12. Web Application Security

Web applications can be exposed to attacks when input, authentication, sessions, or application logic are not handled securely.

Developers should validate input, encode output appropriately, protect sessions, and enforce authorization.

Common web security concerns include injection, cross-site scripting, broken access control, and insecure configuration.

Security testing should be included throughout the software development lifecycle.

13. API Security

APIs allow applications and services to exchange data and perform operations.

API security should include authentication, authorization, input validation, rate limiting, and secure error handling.

Sensitive endpoints should not expose more information or functionality than required.

API keys and tokens should be protected and should not be hard-coded into publicly accessible source code.

14. Endpoint Security

Endpoints include laptops, desktops, mobile devices, servers, and other connected devices.

Endpoint security can include operating-system updates, antivirus or endpoint protection, device controls, and secure configuration.

Unused applications and services should be removed or disabled where appropriate.

Lost or compromised devices should be handled through defined reporting, access-revocation, and recovery procedures.

15. Cloud Security

Cloud security protects applications, data, identities, and infrastructure hosted on cloud platforms.

Organizations must correctly configure access permissions, storage, networks, secrets, and monitoring.

Cloud security follows a shared-responsibility approach in which the provider and customer have different security responsibilities.

Regular configuration reviews help identify excessive permissions and unintended public exposure.

16. Identity and Access Management

Identity and Access Management (IAM) controls who can access systems and what they are allowed to do.

Access should follow the principle of least privilege, giving users and services only the permissions they need.

Roles and permissions should be reviewed as responsibilities change.

Strong identity controls reduce the risk of unauthorized access to applications and data.

17. Secure Software Development

Secure software development integrates security into requirements, design, coding, testing, deployment, and maintenance.

Developers should validate inputs, protect secrets, handle errors safely, and keep dependencies updated.

Code review and security testing can identify vulnerabilities before release.

Security requirements should be considered alongside functionality and performance requirements.

18. Security Monitoring and Incident Detection

Security monitoring collects and analyzes events that may indicate suspicious activity.

Logs can provide useful information about authentication, application errors, network events, and system changes.

Monitoring helps teams detect unusual behavior and investigate potential incidents.

Important logs should be protected from unauthorized modification and should be retained according to organizational requirements.

19. Incident Response and Recovery

Incident response is the organized process of identifying, containing, investigating, and recovering from a security incident.

A basic response process can include preparation, detection, analysis, containment, eradication, recovery, and lessons learned.

Backups can help restore important information after accidental loss, malware, or other incidents.

Organizations should document response procedures and practice them so that teams can act effectively during real incidents.

20. Cyber Security Best Practices

Keep operating systems, applications, libraries, and devices updated with appropriate security fixes.

Use strong authentication and MFA for important accounts.

Apply least-privilege access and remove unnecessary permissions.

Back up important information and test whether backups can actually be restored.

Educate users about phishing, passwords, safe browsing, and incident reporting.

Monitor systems and investigate unusual activity.

- Use defense-in-depth instead of depending on one security control.
- Review permissions and configurations regularly.
- Test security controls and incident-response procedures.
- Document security responsibilities and escalation procedures.

21. Common Cyber Security Mistakes

Do not reuse the same password across important accounts.

Do not store passwords, API keys, or other secrets directly in source code.

Do not give users or applications unnecessary permissions.

Do not ignore software updates and security patches.

Do not assume that a backup is useful without testing recovery.

Do not treat security as only a final testing activity; include it throughout development.

22. Cyber Security in Real World Applications

Cyber security is important in banking systems, healthcare applications, educational platforms, e-commerce websites, cloud services, enterprise portals, mobile applications, and government systems.

Real-world security commonly combines identity management, encryption, network controls, application security, monitoring, backups, and incident response.

Organizations also use security awareness programs and policies to reduce risks caused by human mistakes.

Security controls should be adapted to the system's data, users, business requirements, and risk level.

23. Summary

Cyber security protects digital systems, applications, networks, devices, and information from unauthorized or harmful activity.

Important fundamentals include the CIA triad, authentication, MFA, access control, encryption, network security, secure development, monitoring, and incident response.

Security requires both technical controls and responsible user behavior.

Regular testing, updates, monitoring, backups, and security awareness help organizations reduce cyber risk.

24. Exercises

1. Explain the three parts of the CIA triad with one example for each.
2. Identify five common cyber threats that can affect a web application.
3. Create a checklist for improving password and MFA security for a student account.
4. Design a simple network-security diagram showing users, a firewall, an application server, and a database.
5. List five ways to protect data stored in an application.
6. Identify three security practices that should be followed when developing an API.
7. Create a basic incident-response flow for a suspected phishing attack.
8. Choose a cloud application and list the identities, data, and resources that need protection.
9. Review a sample web application and identify possible authentication, authorization, input-validation, and configuration risks.
10. Prepare a personal cyber-security checklist containing at least ten actions that can reduce everyday security risks.