Information security vs cybersecurity

Information security and cybersecurity are often used interchangeably, but they are not the same thing. Information security is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction. Cybersecurity is a subset of information security that focuses on protecting digital data from unauthorized access, theft, and damage. It is concerned with protecting computer systems and networks from attacks, viruses, and other threats that can compromise the confidentiality, integrity, and availability of data.

incident

An information security incident is an event or situation that has the potential to compromise the confidentiality, integrity, or availability of information. It can be caused by unauthorized access, use, disclosure, data breach, modification, or destruction of information. Examples of information security incidents include theft or loss of equipment containing sensitive information. Security incidents are events that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed¹.

A security event that compromises the confidentiality, integrity, or availability of an information asset.

* Incident (siridha)
* Breach( nandhabe)
* Trademark
* Due care

A patent is a type of intellectual property that gives its owner the legal right to exclude others from making, using, or selling an invention for a limited period of time in exchange for publishing an enabling disclosure of the invention¹.

Copyright is a type of intellectual property that gives its owner the exclusive right to copy, distribute, adapt, display, and perform a creative work, usually for a limited time. The creative work may be in a literary, artistic, educational, or musical form. Copyright is intended to protect the original expression of an idea in the form of a ...

[SQL injection](https://searchsoftwarequality.techtarget.com/definition/SQL-injection) attacks involve attackers inputting SQL code into an application form -- for example, a username or password -- to gain unauthorized access to resources. With this access, attackers can view and alter sensitive data, execute admin privileges, or conduct DDoS and other detrimental attacks.

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. The current version of the OWASP Top 10 is the 2017 version⁴.

OWASP stands for Open Web Application Security Project. It is a nonprofit foundation that works to improve the security of software

The OWASP Top 10 Web Application Threats are:

1. Injection

2. Broken Authentication and Session Management

3. Cross-Site Scripting (XSS)

4. Broken Access Control

5. Security Misconfiguration

6. Insecure Cryptographic Storage

7. Insufficient Transport Layer Protection

8. Unvalidated and Unsanitized Inputs

9. Insufficient Logging and Monitoring

10. Poor Coding Practices².

Sure! Here are the definitions of each risk:

1. Injection Attack - An injection attack occurs when untrusted data is sent to a code interpreter in the form of an input or in some other data submission mode to a web application .

2. Broken Authentication - Broken authentication occurs when an attacker can bypass authentication methods to gain access to sensitive data .

3. Sensitive Data Exposure - Sensitive data exposure occurs when sensitive data is not properly protected and can be accessed by unauthorized users .

4. Broken Access Control - Broken access control occurs when an attacker can bypass access controls to gain access to sensitive data .

5. Security Misconfiguration - Security misconfiguration occurs when security settings are not properly configured and can be exploited by attackers .

6. Cross-Site Scripting (or XSS) - Cross-site scripting (XSS) occurs when an attacker injects malicious code into a web page viewed by other users .

7. Insecure Deserialization - Insecure deserialization occurs when an attacker can manipulate serialized objects to execute arbitrary code .

8. Insufficient Logging & Monitoring - Insufficient logging and monitoring occurs when logs are not properly monitored and attackers can go undetected .

9. Server-Side Request Forgery (SSRF) - Server-side request forgery (SSRF) occurs when an attacker can send requests from a server to other servers on the same network .

10. Using Components with Known Vulnerabilities - Using components with known vulnerabilities occurs when outdated or vulnerable components are used in web applications .

A web application firewall (WAF) is a type of firewall that protects web applications and APIs by filtering, monitoring and blocking malicious web traffic and application-layer attacks — such as DDoS, SQL injection, cookie manipulation, cross-site scripting (XSS), cross-site forgery and file inclusion [1](https://www.paloaltonetworks.com/cyberpedia/what-is-a-web-application-firewall). It is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service

DDoS stands for Distributed Denial of Service. It is a type of cyber attack where multiple compromised systems are used to target a single system or network with the intent of overwhelming it with traffic .

Cross-site scripting (XSS) is a type of security vulnerability that can be found in some web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.

There are three types of XSS attacks: \*\*Reflected XSS\*\*, \*\*Stored XSS\*\*, and \*\*DOM-based **XSS\*\* .**

**- Reflected XSS attacks** occur when an attacker injects malicious code into a website's search field or other input fields that are then reflected back to the user.

**- Stored XSS attacks** occur when an attacker injects malicious code into a website's database that is then served to all users who access the website.

- **DOM-based XSS attacks** occur when an attacker injects malicious code into a website's Document Object Model (DOM) that is then executed by the user's browser .

Automated pen testing tools can pick up vulnerabilities that may be missed by manual code reviews. These include:

- \*\*Memory leaks\*\* that can cause a system to crash or become unstable.

- \*\*Buffer overflows\*\* that can allow attackers to execute arbitrary code on a system.

- \*\*SQL injection\*\* vulnerabilities that can allow attackers to access sensitive data.

- \*\*Cross-site scripting (XSS)\*\* vulnerabilities that can allow attackers to inject malicious code into web pages viewed by other users.

- \*\*Cross-site request forgery (CSRF)\*\* vulnerabilities that can allow attackers to execute unauthorized actions on behalf of a user.

Manual code reviews are performed by human reviewers who examine the source code of an application line by line to identify potential vulnerabilities. Automated pen testing tools, on the other hand, use software to scan an application for vulnerabilities. While manual code reviews can be more thorough and can identify more complex vulnerabilities, they can also be time-consuming and expensive. Automated pen testing tools can quickly identify common vulnerabilities and can be run more frequently than manual code reviews .

Here are ten MCQs on information or computer security:

1. Which of the following is not a type of malware?

a. Virus

b. Worm

c. Trojan horse

d. Firewall

2. Which of the following is not a type of cyber attack?

a. Phishing

b. Malware

c. Social engineering

d. Encryption

3. Which of the following is not a type of social engineering attack?

a. Phishing

b. Spear phishing

c. Malware

d. Baiting

4. Which of the following is not a type of access control?

a. Mandatory access control (MAC)

b. Discretionary access control (DAC)

c. Role-based access control (RBAC)

d. Firewall-based access control

5. Which of the following is not a type of encryption?

a. Symmetric-key encryption

b. Asymmetric-key encryption

c. Hashing

d. Firewall-based encryption

6. Which of the following is not a type of authentication?

a. Password authentication

b. Biometric authentication

c. Firewall-based authentication

d. Multi-factor authentication

7. Which of the following is not a type of network security?

a. Firewall security

b. Intrusion detection and prevention systems (IDPS)

c. Virtual private network (VPN) security

d. Social engineering security

8. Which of the following is not a type of vulnerability assessment?

a. Penetration testing

b. Vulnerability scanning

c. Social engineering testing

d. Risk assessment

9. Which of the following is not a type of security policy?

a. Acceptable use policy (AUP)

b. Password policy

c. Firewall policy

d. Remote access policy

10.Which of the following is not a type of backup?

a.Full backup

b.Incremental backup

c.Differential backup

d.Firewall backup

Here are the answers to the MCQs:

1. d. Firewall

2. d. Encryption

3. c. Malware

4. d. Firewall-based access control

5. d. Firewall-based encryption

6. c. Firewall-based authentication

7. d. Social engineering security

8. c. Social engineering testing

9. c. Firewall policy

10.d. Firewall backup

There are several types of vulnerability assessment. Here are some of them:

1. Host vulnerability assessment (HBVA): Identifies and evaluates the vulnerabilities of hosts on a network.

2. Database vulnerability assessments: Identifies vulnerabilities in databases.

3. Application vulnerability assessments: Identifies security vulnerabilities in applications.

4. Social engineering vulnerability assessments: Identifies vulnerabilities in human behavior.

5. Network vulnerability assessment: Identifies possible network security issues and can detect vulnerable systems on wired and wireless networks.

6. Cloud security assessment: Identifies vulnerabilities in cloud-based systems.

There are different types of security policies. Here are some of them:

1. Technical security policies: Describe the configuration of the technology for convenient use.

2. Administrative security policies: Address how all persons should behave.

There are also three main types of policies that exist according to [Sage-Advices- Organizational (or Master) Policy.

- System-specific Policy.

- Issue-specific Policy.

**Technical security policies** describe the configuration of the technology for convenient use. They are designed to protect the confidentiality, integrity, and availability of information systems. Technical security policies can include password policies, access control policies, and encryption policies.

**Administrative security policies** address how all persons should behave. They encompass a wide range of approaches, including formal policies, procedural guidelines, risk mitigation strategies, and training activities.

Security policies aim to ensure right-action among employees, keeping systems safe by promoting desired behavior or preventing undesirable actions. Below are a few examples of some of the administrative security policies in place at many companies according to [Firewall Times](https://firewalltimes.com/administrative-security-controls/):

- Password Policies: A password policy sets requirements for the use of passwords, including complexity standards, change...

- Access Control Policies: An access control policy outlines rules regarding who can access various resources within an...

- Data Collection Policies: Data ...

Here are 10 multiple choice questions on attacks:

1. What is the most common type of cyber attack?

A. Malware

B. Phishing

C. Denial-of-service (DoS) attack

D. SQL injection

2. What is a phishing attack?

A. A type of malware that encrypts files on a computer

B. A type of social engineering attack that tricks users into giving away sensitive information

C. A type of denial-of-service (DoS) attack that floods a network with traffic

D. A type of attack that exploits vulnerabilities in web applications

3. What is a man-in-the-middle (MitM) attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. An attack that floods a network with traffic

D. A type of social engineering attack that tricks users into giving away sensitive information

4. What is a distributed denial-of-service (DDoS) attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. An attack that floods a network with traffic from multiple sources

D. A type of social engineering attack that tricks users into giving away sensitive information

5. What is a SQL injection attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. A type of social engineering attack that tricks users into giving away sensitive information

D. A type of malware that encrypts files on a computer

6. What is a cross-site scripting (XSS) attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. A type of social engineering attack that tricks users into giving away sensitive information

D. A type of malware that encrypts files on a computer

7. What is an Advanced Persistent Threat (APT)?

A. A type of malware that encrypts files on a computer

B. A type of social engineering attack that tricks users into giving away sensitive information

C. A long-term targeted cyberattack aimed at stealing data or intellectual property from an organization or government agency.

D. A type of denial-of-service (DoS) attack that floods a network with traffic

8. What is ransomware?

A. A type of malware that encrypts files on a computer and demands payment for their release.

B. A type of social engineering attack that tricks users into giving away sensitive information.

C. A long-term targeted cyberattack aimed at stealing data or intellectual property from an organization or government agency.

D. A type of denial-of-service (DoS) attack that floods a network with traffic.

9.What is an insider threat?

A.A threat posed by an external attacker.

B.A threat posed by an employee or contractor with access to an organization's systems and data.

C.A threat posed by an attacker who has gained access to an organization's systems and data through social engineering.

D.A threat posed by an attacker who has gained access to an organization's systems and data through exploiting vulnerabilities.

10.What is the difference between black hat hackers and white hat hackers?

A.Black hat hackers are ethical hackers who work for organizations to find vulnerabilities in their systems.

B.White hat hackers are unethical hackers who use their skills for personal gain.

C.Black hat hackers are unethical hackers who use their skills for personal gain.

D.White hat hackers are ethical hackers who work for organizations to find vulnerabilities in their systems.

Here are 10 multiple choice questions on attacks:

1. What is the most common type of cyber attack?

A. Malware

B. Phishing

C. Denial-of-service (DoS) attack

D. SQL injection

2. What is a phishing attack?

A. A type of malware that encrypts files on a computer

B. A type of social engineering attack that tricks users into giving away sensitive information

C. A type of denial-of-service (DoS) attack that floods a network with traffic

D. A type of attack that exploits vulnerabilities in web applications

3. What is a man-in-the-middle (MitM) attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. An attack that floods a network with traffic

D. A type of social engineering attack that tricks users into giving away sensitive information

4. What is a distributed denial-of-service (DDoS) attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. An attack that floods a network with traffic from multiple sources

D. A type of social engineering attack that tricks users into giving away sensitive information

5. What is a SQL injection attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. A type of social engineering attack that tricks users into giving away sensitive information

D. A type of malware that encrypts files on a computer

6. What is a cross-site scripting (XSS) attack?

A. An attack that exploits vulnerabilities in web applications

B. An attack that intercepts communication between two parties

C. A type of social engineering attack that tricks users into giving away sensitive information

D. A type of malware that encrypts files on a computer

7. What is an Advanced Persistent Threat (APT)?

A. A type of malware that encrypts files on a computer

B. A type of social engineering attack that tricks users into giving away sensitive information

C. A long-term targeted cyberattack aimed at stealing data or intellectual property from an organization or government agency.

D. A type of denial-of-service (DoS) attack that floods a network with traffic

8. What is ransomware?

A. A type of malware that encrypts files on a computer and demands payment for their release.

B. A type of social engineering attack that tricks users into giving away sensitive information.

C. A long-term targeted cyberattack aimed at stealing data or intellectual property from an organization or government agency.

D. A type of denial-of-service (DoS) attack that floods a network with traffic.

9.What is an insider threat?

A.A threat posed by an external attacker.

B.A threat posed by an employee or contractor with access to an organization's systems and data.

C.A threat posed by an attacker who has gained access to an organization's systems and data through social engineering.

D.A threat posed by an attacker who has gained access to an organization's systems and data through exploiting vulnerabilities.

10.What is the difference between black hat hackers and white hat hackers?

A.Black hat hackers are ethical hackers who work for organizations to find vulnerabilities in their systems.

B.White hat hackers are unethical hackers who use their skills for personal gain.

C.Black hat hackers are unethical hackers who use their skills for personal gain.

D.White hat hackers are ethical hackers who work for organizations to find vulnerabilities in their systems.

There are three main types of hackers: white hat hackers, black hat hackers, and grey hat hackers¹²³.

**White hat hackers** are ethical hackers who work for organizations to find vulnerabilities in their systems. They are authorized or certified hackers who perform penetration testing and identify loopholes in cybersecurity⁴.

**Black hat hackers** are unethical hackers who use their skills for personal gain. They break into computer systems with malicious or criminal intent⁵.

**Grey hat hackers** are a combination of both white and black hat hackers. They may break into computer systems without permission but do not have malicious intent. Instead, they may do so to expose vulnerabilities and help organizations improve their security¹.

There are several principles, methods and technologies that can be used to make software more secure. **One** such method is the Secure Development Lifecycle (SDL), which is a set of development practices for strengthening security and compliance. These practices should be integrated into all stages of software development and maintenance².

**Other principles of IT security include** confidentiality, integrity, availability, authentication, authorization, and non-repudiation³.

**Some practical steps** that can be taken to improve data security include backing up data regularly, encrypting external storage devices, and keeping them somewhere other than the main workplace⁴.

Here are some practical steps you and your staff can take to improve your data security.

1. Back up your data

You **should** back up your data regularly. If you’re using an external storage device, keep it somewhere other than your main workplace – encrypt it, and lock it away if possible. That way, if there’s a break-in, fire or flood, you’ll minimise the risk of losing all your data.

Check your back-up. You don’t want to find out it’s not worked when you need it most. Make sure your back-up isn’t connected to your live data source, so that any malicious activity doesn’t reach it.

2. Use strong passwords and multi-factor authentication

Make sure you use strong passwords on smartphones, laptops, tablets, email accounts and any other devices or accounts where personal information is stored. They **must** be difficult to guess. The National Cyber Security Centre (NCSC) recommends using [three random words](https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words).

Where possible, you should consider using multi-factor authentication. Multi-factor authentication is a security measure to make sure the right person is accessing the data. It requires at least two separate forms of identification before access is granted. For example, you use a password and a one-time code which is sent by text message.

3. Be aware of your surroundings

For example, if you’re on a train or in a shared workspace, other people may be able to see your screen. A privacy screen might help you.

4. Be wary of suspicious emails

You and your staff need to know how to spot suspicious emails. Look out for signs such as bad grammar, demands for you to act urgently and requests for payment. New technologies mean that email attacks are becoming more sophisticated. A phishing email could appear to come from a source you recognise. If you’re not sure, speak to the sender. NCSC provide useful [training materials](https://www.youtube.com/watch?v=NhaPVefCjDo) to help you and your staff recognise suspicious emails.

5. Install anti-virus and malware protection

And keep it up-to-date.

You **must** make sure the [devices you and your employees use at home, or when you’re working away, are secure](https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/working-from-home/bring-your-own-device-what-should-we-consider/). Anti-virus software can help protect your device against malware sent through a phishing attack.

6. Protect your device when it’s unattended

Lock your screen when you’re temporarily away from your desk to prevent someone else accessing your computer. If you do need to leave your device for longer, put it in a secure place, out of sight.

7. Make sure your Wi-Fi connection is secure

Using public Wi-Fi, or an insecure connection, could put personal data at risk. You **should** make sure you always use a secure connection when connecting to the internet. If you’re using a public network, consider using a secure Virtual Private Network (VPN).

8. Limit access to those who need it

Different workers may need to use different types of information. Put access controls in place to make sure people can only see the information they need. For example, payroll or HR may need to see workers’ personal information, but your sales staff won’t.

If someone leaves your company, or if they’re absent for a long period of time, suspend their access to your systems.

9. Take care when sharing your screen

Sharing your screen in a virtual meeting may show your device to others exactly as you see it, including any open tabs or documents. Before sharing your screen, you **should** close anything you don’t need and make sure your notifications and pop-up alerts are switched off.

10. Don’t keep data for longer than you need it

Getting rid of data you no longer need will free up storage space. This also means you have less personal information at risk if you suffer a cyber-attack or personal data breach.

11. Dispose of old IT equipment and records securely

You **must** make sure no personal data is left on computers, laptops, smartphones or any other devices, before you dispose of them. You **could** consider using deletion software, or hire a specialist to wipe the data.

**There are several threats that can make software less secure**. Some of the most common ones include malware, unpatched security vulnerabilities, hidden backdoor programs, superuser or admin account privileges, automated running of scripts without malware/virus checks, unknown security bugs in software or programming interfaces, and phishing (social engineering) attacks¹.

Sure! Here are some definitions:

- \*\***Malware\*\*** is short for "malicious software." It is a type of software designed to harm or exploit any programmable device, service, or network.

**- \*\*Phishing\*\*** is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

**- A \*\*backdoor program\*\*** is a method of bypassing normal authentication procedures to gain access to a computer system or encrypted data.

**- A \*\*superuser\*\*** is a user account with privileges that allow them to perform tasks that are not available to other users.

- **An \*\*admin account\*\*** is an account with administrative privileges that allow the user to perform tasks that are not available to other users.

- \*\***SQL injection attacks\*\*,** which exploit vulnerabilities in web applications that use SQL databases.

**- \*\*Cross-site scripting (XSS)\*\*** attacks, which exploit vulnerabilities in web applications that allow attackers to inject client-side scripts into web pages viewed by other users.

Cross-site scripting (XSS) is a type of security vulnerability that allows attackers to inject client-side scripts into web pages viewed by other users. This can allow attackers to steal data or take control of the victim’s browser.

**- \*\*Man-in-the-middle (MITM)\*\*** attacks, which occur when an attacker intercepts communication between two parties to steal data or inject malware.

**- \*\*Denial-of-service (DoS)\*\*** attacks, which occur when an attacker floods a network or server with traffic to disrupt normal operations.

**There are many vulnerabilities that can make software less secure**. Some of the most common ones include:

- \*\***Buffer overflow vulnerabilities\*\*,** which occur when a program tries to store more data in a buffer than it was designed to hold.

Buffer overflow is a type of software vulnerability that occurs when a program tries to store more data in a buffer than it was designed to hold. This can cause the program to crash or allow attackers to execute arbitrary code on the system.

**Here are some ways to protect yourself from buffer overflow:**

- \*\*Use a programming language that provides built-in memory management\*\*, such as Java or Python.

- \*\*Use a compiler that provides buffer overflow protection\*\*, such as Microsoft's Visual C++.

- \*\*Use a static analysis tool\*\* to detect buffer overflow vulnerabilities in your code.

- \*\*Use a runtime analysis tool\*\* to detect buffer overflow vulnerabilities in your running code.

- **\*\*Race conditions\*\*,** which occur when two or more processes or threads access shared data at the same time.

- \*\***Privilege escalation vulnerabilities\*\*,** which allow attackers to gain elevated privileges on a system.

- \*\***Insecure communication protocols\*\*,** which can allow attackers to intercept and modify data in transit.

**-\*\*Broken authentication and session management\*\***: This occurs when an application fails to properly authenticate users or manage their sessions

**Secure coding practices entail writing code in a way that will prevent potential security vulnerabilities.** This includes maintaining both your source code and any third-party libraries in a secure state. Some examples of secure coding practices include:

- \*\*Input validation\*\*: This involves validating all input data to ensure that it is of the expected type and within the expected range¹.

- \*\*Output encoding\*\*: This involves encoding all output data to prevent cross-site scripting (XSS) attacks¹.

- \*\*Authentication and authorization\*\*: This involves properly authenticating users and authorizing them to access only the resources they need¹.

- \*\*Error handling\*\*: This involves handling errors in a way that does not reveal sensitive information¹.

There are many other secure coding practices that developers can follow to help prevent security vulnerabilities. Some resources that may be helpful include:

- The \*\*Open Web Application Security Project (OWASP)\*\* provides a wealth of information on secure coding practices, including a [Secure Coding Practices Quick Reference Guide](https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/) ⁴.

- \*\*Snyk\*\* provides a list of [5 best practices for your secure coding checklist](https://snyk.io/learn/secure-coding-practices/) ¹.

- \*\*Ksolves\*\* provides a list of the [top 10 best secure coding practices](https://www.ksolves.com/blog/penetration-testing/top-10-best-secure-coding-practices) ³.

Sure! Here are the 5 best practices for your secure coding checklist provided by Snyk:

1. \*\*Code minification and obfuscation\*\*: Making your code harder to access, and by extension harder to read, can deter attackers from trying to exploit it.

2. \*\*Avoiding shortcuts\*\*: It can be tempting for developers to want to take shortcuts to release code into production faster, but this can lead to security vulnerabilities.

3. \*\*Automated testing\*\*: Automated testing can help identify security vulnerabilities before they become a problem.

4. \*\*Keeping dependencies up-to-date\*\*: Outdated dependencies can contain known security vulnerabilities that attackers can exploit.

5. \*\*Using a web application firewall (WAF)\*\*: A WAF can help protect your application from common attacks like SQL injection and cross-site scripting (XSS).

**Here are the top 10 best secure coding practices provided by Ksolves:**

1. \*\*Input validation\*\*: This involves validating all input data to ensure that it is of the expected type and within the expected range.

2. \*\*Output encoding\*\*: This involves encoding all output data to prevent cross-site scripting (XSS) attacks.

3. \*\*Authentication and authorization\*\*: This involves properly authenticating users and authorizing them to access only the resources they need.

4. \*\*Session management\*\*: This involves properly managing user sessions to prevent session hijacking attacks.

5. \*\*Error handling and logging\*\*: This involves handling errors in a way that does not reveal sensitive information and logging errors for analysis.

6. \*\*Secure communication\*\*: This involves using secure communication protocols like HTTPS to protect data in transit.

7. \*\*Secure storage\*\*: This involves storing sensitive data securely, such as using encryption or hashing algorithms.

8. \*\*Secure configuration management\*\*: This involves properly configuring servers and applications to prevent security vulnerabilities.

9. \*\*Secure coding practices\*\*: This involves following best practices for writing secure code, such as avoiding buffer overflows and SQL injection attacks.

10. \*\*Regular security audits\*\*: This involves regularly auditing your application for security vulnerabilities and addressing any issues that are found.

**Session hijacking** is a type of attack where an attacker takes over a user's session on a website or application. This can allow the attacker to perform actions on behalf of the user, such as making purchases or changing account settings. To prevent session hijacking attacks, developers can use techniques such as:

- \*\*Session timeouts\*\*: This involves automatically logging users out after a certain period of inactivity.

- \*\*Secure session IDs\*\*: This involves using secure session IDs that are difficult to guess or brute-force.

- \*\*HTTPS\*\*: This involves using HTTPS to encrypt data in transit and prevent attackers from intercepting session cookies.

**HTTPS** stands for Hypertext Transfer Protocol Secure. It is a protocol for secure communication over the internet. HTTPS encrypts data in transit between a user's web browser and a website to prevent attackers from intercepting sensitive information such as passwords or credit card numbers. Websites that use HTTPS have a padlock icon in the address bar of the web browser.

**SSL** stands for Secure Sockets Layer. It is a security protocol that provides encryption and authentication for internet communications. SSL was first developed by Netscape in 1995 for the purpose of ensuring privacy, authentication, and data integrity in Internet communications¹. SSL is the predecessor to the modern TLS encryption used today¹.

**TLS** stands for Transport Layer Security. It is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website³. TLS aims primarily to provide security, including privacy (confidentiality), integrity, and authenticity through the use of cryptography, such as the use of certificates, between two or more communicating computer applications².

Cyber Criminals

Who are Cyber Criminals? It can be anyone, but let us discuss some common ones we see in the media all the time:

* State-sponsored groups targeting organizations in other countries
* Hacking Groups out to target companies to make them pay ransom
* Kids in their rooms doing illegal hacking

**Note:** Cryptocurrency is money represented in digital form instead of physical. There are many different Cryptocurrencies, some very widespread like Bitcoin, and others smaller and unknown to most people. These currency models relies on strong cryptography and public ledger systems to keep track of transactions and how much currency is on the market.