**Passive voice**

**Exercise 1: Rewrite the following sentences in the passive voice.**

1. Hackers attack thousands of websites every day.

-Thousands of websites were attacked by hackers every day

1. Developers implement security protocols to protect user data.

-The user data was protected for the developers implement security protocols

1. The company updated the firewall last week.

-The last week were updated the firewall for the company

1. Cybercriminals stole sensitive information from the database.

-Sensitive information from database was stolen

1. The IT department will install a new antivirus next month.

-The next month will be installed a new antivirus by IT department

1. The software engineers designed a new authentication system.

-A new authentication system was designed by software engineers.

1. Someone accessed the server without permission.

-The server was accessed by someone without permission.

1. The security team is analysing the latest cyber-attack.

-The latest cyber-attack is being analysed by security team.

1. The organization has launched a new cybersecurity campaign.

-A new cybersecurity campaign had been launched by organization.

1. The government will introduce stricter data protection laws.

-Stricter data protection laws will be introduced by the government.

**Exercise 2: Complete the sentences using the correct passive form of the verbs in parentheses.**

1. Personal data \_is\_stolen\_ (steal) by hackers if the website is not secure.
2. A security patch \_\_was released\_\_\_ (release) last week to fix the vulnerability.
3. Two-factor authentication \_wis\_recommended\_\_\_ (recommend) by experts to enhance security.
4. The database \_was encrypted\_\_\_\_ (encrypt) before it was uploaded to the server.
5. A new security policy will\_be\_introduced\_\_\_\_ (introduce) next year to prevent cyber-attacks.
6. Unauthorized access \_was\_detected\_\_\_ (detect) by the monitoring system.
7. The phishing email \_\_was\_sent\_\_ (send) to thousands of users yesterday.
8. Security measures\_are\_implemented\_\_ (implement) to protect customer transactions.
9. Several security breaches \_had been reported\_\_ (report) in the last three months.
10. All login attempts \_are\_logged\_ (log) automatically by the system.

**Exercise 3: Identify whether the following sentences are in the active or passive voice. Then, rewrite the active sentences in the passive voice.**

1. A firewall was installed to protect the network. (PV)
2. The system encrypts all passwords automatically. (A.V)

P.V: All passwords are encrypted by the system

1. The new security update has been deployed by the IT team. (P.V)
2. Cybercriminals frequently exploit software vulnerabilities. (A.V)

P.V: Software vulnerabilities are frequently exploited by cybercriminals.

1. Multi-factor authentication is used to verify user identity. (P.V)
2. Developers will implement stricter security protocols. (A.V)

P.V: Stricter security protocols will be implemented by developers.

1. A report about cybersecurity threats was published last month. (P.V)
2. The company stores all user credentials in an encrypted format. (A.V)

P.V: All user credentials are stored in an encrypted format by the company

1. The personal data of millions of users has been leaked online. (P.V)
2. Security awareness training is provided to all employees. .(P.V)

**Exercise 4: Rearrange the words to form correct passive sentences.**

1. website / hacked / last night / was / the

The website was hacked last night.

1. new / implemented / a / security system / was

A new security system was implemented

1. user accounts / deleted / accidentally / were

User accounts were accidentally deleted.

1. encrypted / passwords / all / are / automatically

All passwords are encrypted automatically.

1. will / new policies / introduced / be / next year

New policies will be introduced next year.

1. by / the / cyber-attack / was / security team / investigated

The cyber-attack was investigated by the security team

1. was / the / updated / last week / firewall

The firewall was updated last week

1. are / automatically / emails / filtered / spam

Emails are filtered automatically for spam

1. detected / unusual activity / system / the / by / was

Unusual activity was detected by the system.

1. affected / many / by / the / were / data breach / users

Many users were affected by the data breach

**Exercise 5: Rewrite the sentences in the indicated tense using the passive voice.**

1. (Present Simple) The company monitors all login attempts.

All login attempts are monitored by the company

1. (Past Simple) The hacker accessed confidential files.

Confidential files were accessed by the hacker.

1. (Present Perfect) The IT team has fixed the security breach.

The security breach has been fixed by the IT team.

1. (Future Simple) They will update the security policy soon.

The security policy will be updated soon

1. (Modal: must) Developers must follow strict security guidelines.

Strict security guidelines must be followed by developers

1. (Past Continuous) The security team was analysing the attack when the system crashed.

The attack was being analysed by the security team when the system crashed.

1. (Future Perfect) By next year, the organization will have implemented new security measures.

By next year, new security measures will have been implemented by the organization

1. (Present Continuous) The company is installing new firewalls across all servers.

New firewalls are being installed across all servers by the company.

1. (Past Perfect) The cybercriminals had stolen data before the breach was detected.

Data had been stolen by the cybercriminals before the breach was detected.

1. (Modal: should) All passwords should be changed regularly.

All passwords should be changed regularly.

**Exercise 6: Each of the following sentences contains an error in the use of the passive voice. Identify and correct the mistake.**

1. A new firewall was install last week to improve security.

\*intalled

1. The sensitive data is encrypted by the developers yesterday.

\*was

1. A cyber attack detected was by the security team.

\*was detected

1. The security protocols are be updated every month.

\*are update

1. Unauthorized access will prevented by strong authentication methods.

\*will be

1. The malware has deleted been from the infected systems.

\*has been deleted

1. A phishing email was send to all employees.

\*was sent

1. All user accounts should monitored for suspicious activity.

\*should be

1. The database was being update when the breach happened.

\*updated

1. Personal information is stole if websites are not secure.

\*stolen