QCERT-CW3

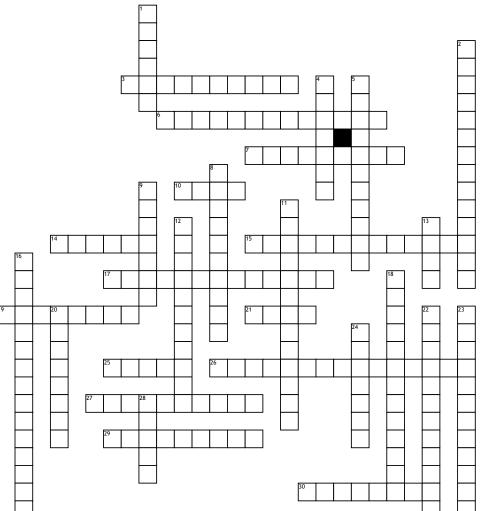## Across

3. An action when a person tags along with another person who is authorized to gain entry into a restricted area or pass a certain checkpoint.

6. The use of electronic communication to bully a person

7. You entered your email account credentials and you received and SMS with a code that you have to enter for verification. What is the type of this authentication?

10. A standalone malware computer program that replicates itself in order to spread to other computers.

14. An attempt by hackers to damage or destroy a computer network or system.

15. Used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.

17. the fraudulent practice of using another person's name and personal information in order to obtain credit, loans, etc.

19. A basic security mechanism that consists of a secret word or phrase that must be used to gain access to an account

21. Irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.

25. A government agency in Qatar that handles all reported incidents related to cyber attacks

26. A type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder.

27. Encrypted form of the message being sent

29. ensuring the authenticity of information—that information is not altered, and that the source of the information is genuine

30. A local or restricted communications network, especially a private network created using World Wide Web software.

Down

1. Any malicious computer program which is used to hack into a computer by misleading users of its true intent

2. A person who uses the art of manipulating people to get access to personal information

4. A software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive

5. Gaining unauthorized logical access to sensitive data by circumventing a system's protections

8. A fraudster fabricates a scenario where he/she will impersonate a person of authority to get access to personal information. What type of attack is it?

9. The part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

11. A weakness in computer software

12. An authentication method that uses procedure of different types of security checks.

13. Similar to worms and Trojans but earn their unique name by performing a wide variety of automated tasks on behalf of their master (the cyber criminals) who are often safely located somewhere far across the Internet.

16. a corporate directive that specifies how employees should leave their working space when they leave the office

18. Approval, permission, or empowerment for someone or something to do something

20. A text message tactic in which individuals are tricked into revealing critical financial or personal information

22. ensuring that data is always accessible whenever needed

23. A word used to describe Tailgating

24. A phone call tactic in which individuals are tricked into revealing critical financial or personal information

28. Appears at the beginning of the web-link of a secured website

Word Bank

Cypher Text	Spyware	Worm	Shoulder Surfing	Social Engineer	Vishing
Integrity	Trojan	Spam	Password	Clear Desk Policy	Cyberbullying
ATTACK	HTTPS	Multi Factor	Dark Web	Penetration	Identity Theft
Pretexting	Malicious Code	Piggybacking	Intranet	SMishing	Authorization
Tailgating	Vulnerability	QCERT	Two Factor	Bots	Availability