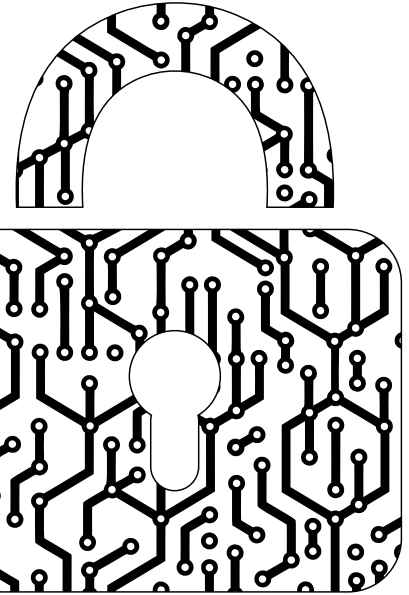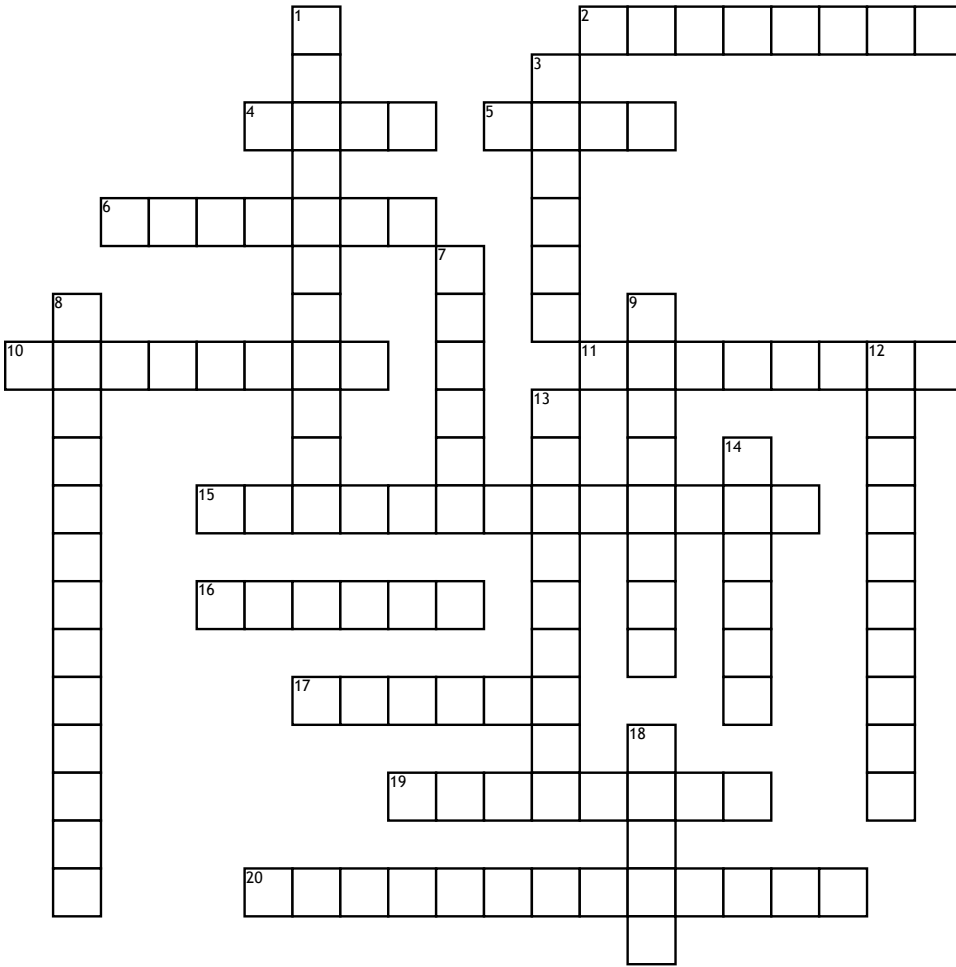# Cyber Security

Across
2. a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.

4. a standalone malware computer program that replicates itself in order to spread to other computers.

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

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

10. a method, often secret, of bypassing normal authentication in a product

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

15. refers to the process of making copies of data or data files to use in the event the original data or data files are lost or destroyed.

16. an attempt by hackers to damage or destroy a computer network or system.

17. someone who seeks and exploits weaknesses in a computer system or computer network.

19. the activity of defrauding an online account holder of financial information by posing as a legitimate company.

20. body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access

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

3. are small files that Web sites put on your computer hard disk drive when you first visit

7. any software program in which advertising banners are displayed while the program is running.

8. 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.

9. global system of interconnected computer networks that use the Internet protocol suite

12. made possible by using algorithms to create complex codes out of simple data, effectively making it more difficult for cyberthieves to gain access to the information

13. designed to detect and destroy computer viruses.

14. refers to the process of making copies of data or data files to use in the event the original data or data files are lost or destroyed.

18. a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data