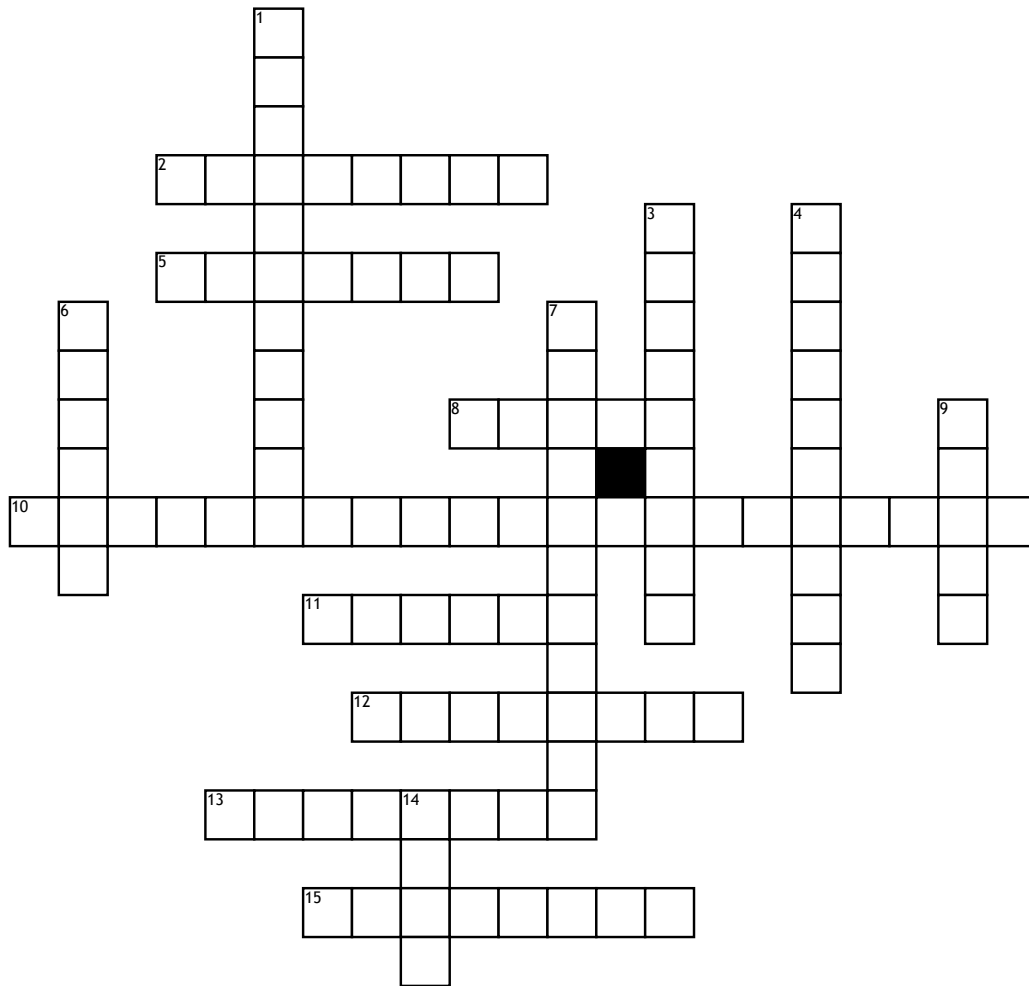


INTERNET SECURITY



Across

2. A technique used by hackers to obtain sensitive information.

5. An umbrella term that describes all forms of malicious software designed to wreak havoc on a computer.

8. A technology that allows us to access our files and/or services through the internet from anywhere in the world.

10. A tool that allows the user to remain anonymous while using the internet by masking the location and encrypting traffic.

11. The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.

12. a global computer network providing a variety of information and communication.

13. A set of programs that tell a computer to perform a task.

15. A defensive technology designed to keep the bad guys out.

Down

1. websites and applications that enable users to create and share content or to participate in social networking.

3. An internet version of a home address for your computer, which is identified when it communicates over a network;

4. The process of encoding data to prevent theft by ensuring the data can only be accessed with a key.

6. A group of computers, printers and devices that are interconnected and governed as a whole.

7. A piece of malware that often allows a hacker to gain remote access to a computer through a "back door".

9. A type of malware aimed to corrupt, erase or modify information on a computer before spreading to others.

14. A piece of malware that can replicate itself in order to spread the infection to other connected computers.

Word Bank

BREACH
MALWARE
FIREWALL
CLOUD
Encryption

INTERNET
SOFTWARE
TROJAN HORSE
WORM
SOCIAL MEDIA

VIRTUAL PRIVATE NETWORK
PHISHING
IP ADDRESS
DOMAIN
VIRUS