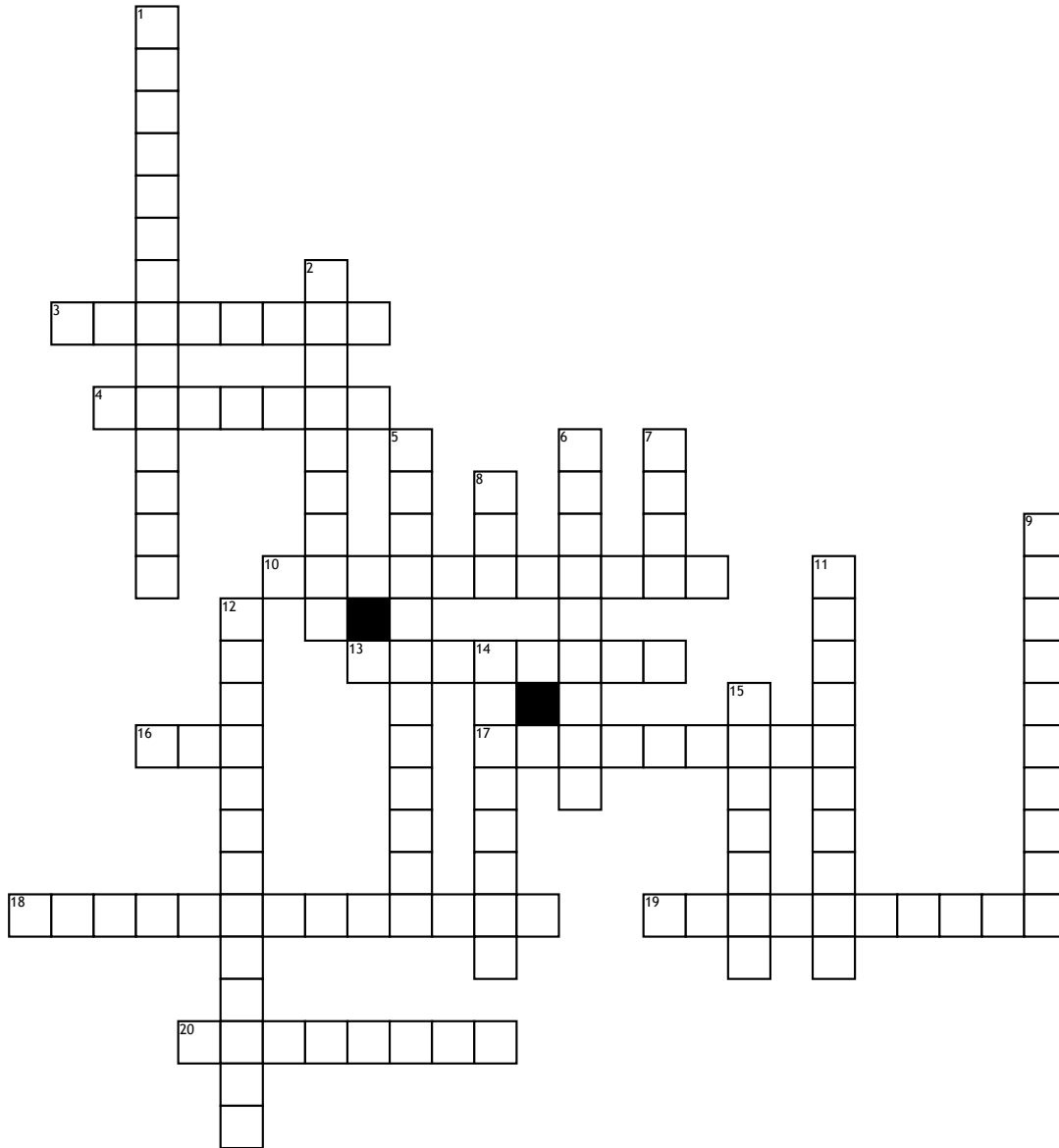


#BeCyberSmart



Across

3. A fraudulent email purportedly from a reputable company attempting to get personal information.
4. Harmful computer programs such as viruses, worms, and trojans used by hackers to gain access to your computer and cause destruction.
10. Facebook, Twitter, Instagram, etc. (Two words)
13. Should be constructed of upper and lower case letters, numbers, and special characters.
16. Security tool that creates a secure, encrypted connection between you and the Internet (acronym).
17. The "I" in the C-I-A Triad; protection from unauthorized changes.
18. Threatening behavior facilitated through electronic means such as texting.

19. A type of malicious software designed to block access to a computer system until a sum of money is paid.
20. Hardware or software designed to prevent unauthorized access to or from a private network.

Down

1. Verifying identity.
2. Unauthorized access to a network, information systems, or application.
5. The "A" in the C-I-A Triad. It ensures authorized users have access.
6. A wireless technology standard used over short distances using short-wavelength UHF radio waves.
7. Widely used in-home network technology that allows for wireless connection in interfacing with the internet.

8. The address of a webpage. Check the validity of it before clicking on it.
9. A sequence of words or text used to control access to a computer; similar to a password.
11. The process of taking plain text and scrambling it into an unreadable format.
12. A flaw or weakness in a computer system that could be exploited to violate the system's security.
14. Fraudulent text messages purporting to be from reputable companies in order to trick individuals into revealing personal information.
15. Fraudulent phone calls or voice messages purporting to be from reputable companies in order to trick individuals into revealing personnel information.