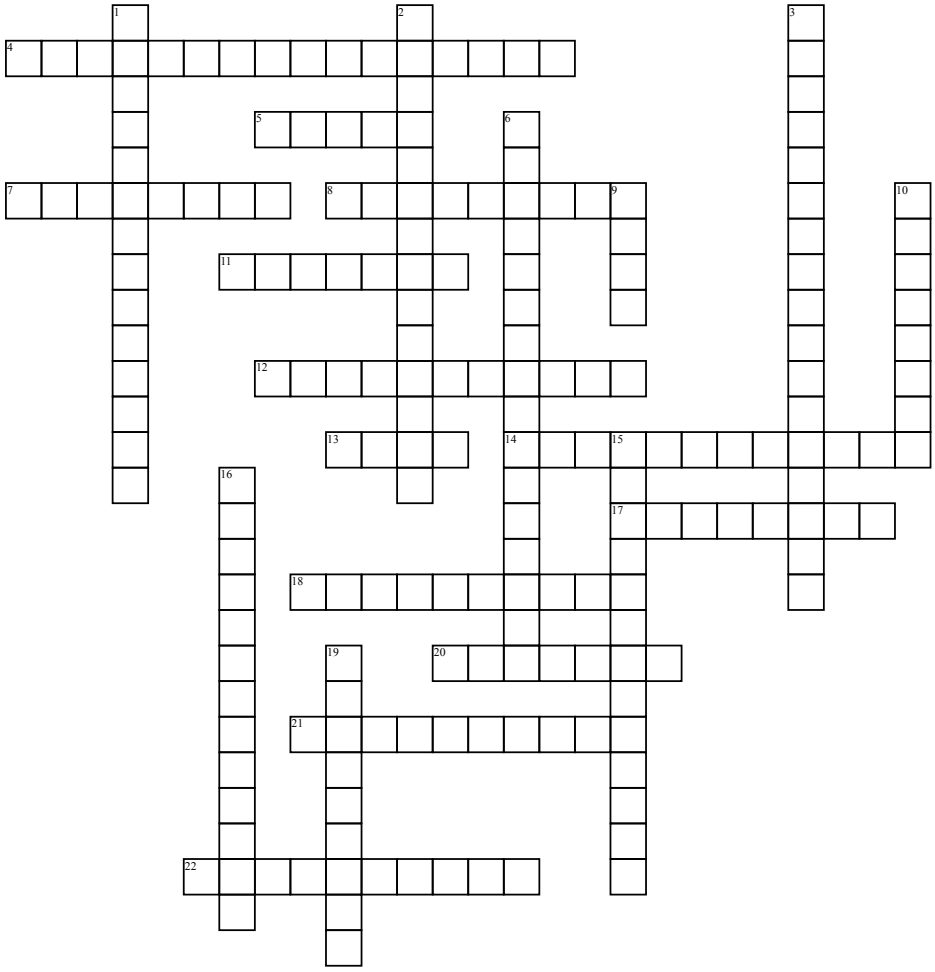
Name: _____

Cyber Awareness Month



Across

4. Identity and Privacy Protection

5. A form of malware that often attaches itself to a host file or the MBR (Master Boot Record) as a parasite. When the host file or MBR is accessed, it activates the virus enabling it to infect other objects. Most viruses spread through human activity within and between computers

7. A security tool, which may be a hardware or software solution that is used to filter network traffic.

8. Someone attempting to create Identity fraud

11. Any code written for the specific purpose of causing harm, disclosing information or otherwise violating the security or stability of a system. Malware includes a wide range of types of malicious programs including: virus, worm, Trojan horse, logic bomb, backdoor, Remote Access Trojan (RAT), rootkit, ransomware and spyware/adware.

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

13. A form of unwanted or unsolicited messages or communications typically received via e-mail but also occurring through text messaging, social networks or VoIP. Most SPAM is advertising, but some may include malicious code, malicious hyperlinks or malicious attachments.

14. Malware is defined as any device software that aims to cause damage and steal data. Malware is an abbreviation for malicious software. Ransomware and trojan, for example, are types of malware widely used in email attacks

17. The act of falsifying the identity of the source of a communication or interaction. It is possible to spoof IP address, MAC address and email address.

18. the ultimate call control center that gives customers full control of all T-Mobile's scam protection options.

20. A form of malware that monitors user activities and reports them to an external their party. Spyware can be legitimate in that it is operated by an advertising and marketing agency for the purpose of gathering customer demographics. However, spyware can also be operated by attackers using the data gathering tool to steal an identity or learn enough about a victim to harm them in other ways.

21. The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment. Generally, a data breach results in internal data being made accessible to external entities without authorization.

22. Something that shows up in a email

Down

1. Hard to detect both by Users

2. The likelihood or potential that an outside entity, such as an ex-employee, competitor or even an unhappy customer, may pose a risk to the stability or security of an organization. An outsider must often gain logical or physical access to the target before launching malicious attacks.

3. An attack focusing on people rather than technology

6. a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and .

9. a dishonest scheme; a fraud.

10. Alerts used as a warning of danger.

15. he likelihood or potential that an employee or another form of internal personnel may pose a risk to the stability or security of an organization

16. A form of identity theft in which a transaction, typically financial, is performed using the stolen identity of another individual. The fraud is due to the attacker impersonating someone else.

19. A security mechanism prohibiting the execution of those programs on a known malicious or undesired list of software