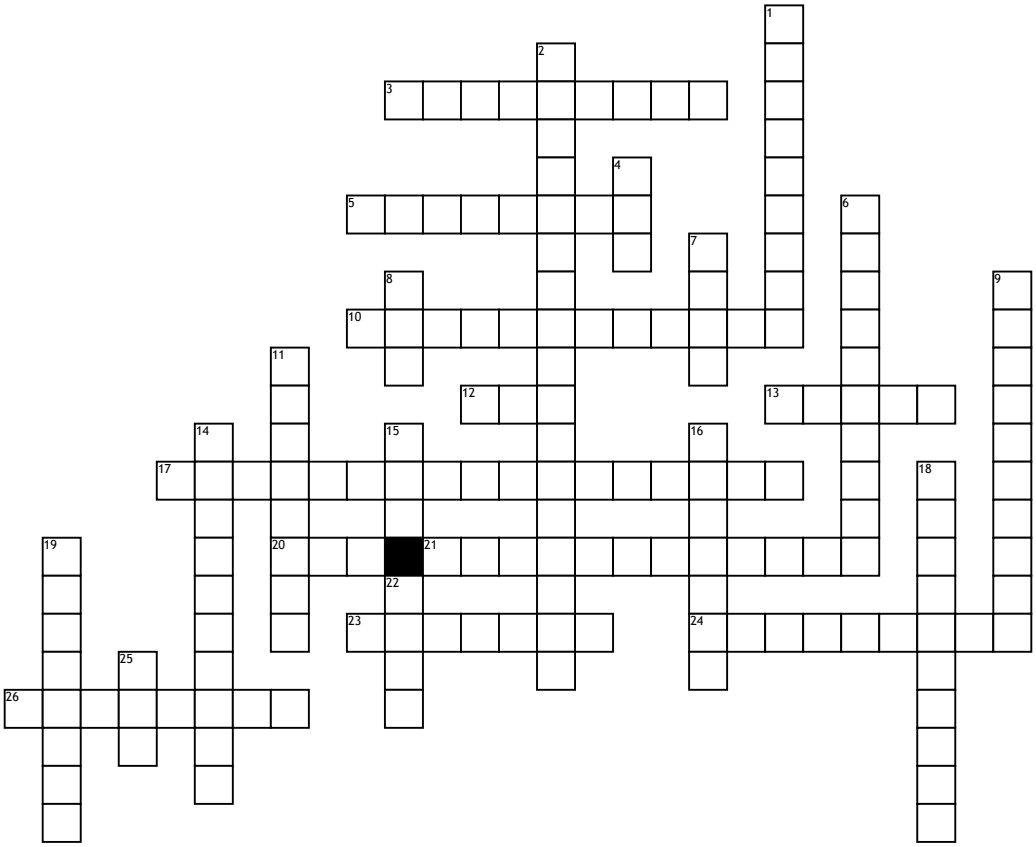
Name: _____ Date: _____

CYBER AWARENESS CROSSWORD



Across

3. Phony email, usually an alert about a non-existent threat, that is passed throughout a system by a large number of individuals who believe it to be true – and that overwhelms the system as a result

5. Accessing a secure network by changing the remote computer's IP address to that of a computer with special privileges; often used in DDoS attacks

10. Making small, undetectable changes over an extended period of time; "penny shaving" is a type of salami attack

12. Interruption in an authorised user's access to a computer network, typically with malicious intent. A DOS attack is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet or the organisation's Intranet.

13. A software update comprised code inserted (or patched) into the code of an executable program.

17. Changing the appearance of a website and/or reducing its usability, usually by replacing the legitimate website with a phony one

20. A system that monitors a network for malicious activities such as security threats or policy

21. A hacker gains access to a group of computers and then uses them to carry out a variety of attacks on other computers

23. Tricking a user (through an email or phone call) into entering credit card information into a bogus voice response system; information entered into the phony system is captured for fraudulent purposes

24. Scam software that appears to be legitimate, to encourage download

26. Redirecting users from a legitimate site to a bogus one; information entered on the phony site is captured for fraudulent purposes

Down

1. Cross-site scripting attack. Malware injected into a trusted site, presented through a hyperlink

2. The ability of the anti-virus software to detect patterns of behavior on the machine

4. A software program that provides cryptographic privacy and authentication for data communication.

6. Distributed denial of service attack. Flooding a network or website or network with requests, making it impossible for legitimate users to access the site

7. A message authentication code that makes use of a cryptographic key along with a hash function.

8. An agreement between two or more entities to allow access to data or information. Details the controls that are to be put in place to protect the data, including how the data will be used, stored, shared and disposed of.

9. Restricts access to a computer; owner must pay ransom to have it removed

11. Phishing using text messages rather than emails

14. Recording the keystrokes made by an authorized user

15. A cipher selected as an official Federal Information Processing Standard (FIPS) for the United States in 1976, and which has subsequently enjoyed widespread use internationally. The algorithm is a sixteen round block cipher which uses a 64bit block and a 56bit key.

16. The security-oriented probing of a computer system or network to seek out vulnerabilities

18. Cross-site request forgery (or "sea-surf") attack. Malware from someone who appears to be a trusted user of a site

19. Directing users to a bogus site through an email that appears legitimate; information entered on the phony site is captured for fraudulent purposes

22. A set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies. (United States of America Federal.)

25. A documented process or set of procedures to recover and protect a business IT infrastructure in the event of a disaster. Such a plan, ordinarily documented in written form, specifies procedures the organisation is to follow in the event of a disaster.

Word Bank

Salami attack	HMAC	IPS	Spoofing	Hoax email
DAA	Botnet attack	DES	XXS attack	FIPS
PGP	Ransomware	DOS	Vishing	XSRF attack
Scareware	Pen Test	Phishing	DDoS attack	Patch
Pharming	Heuristic Scanning	DRP	Smishing	Website defacement
Key logging				