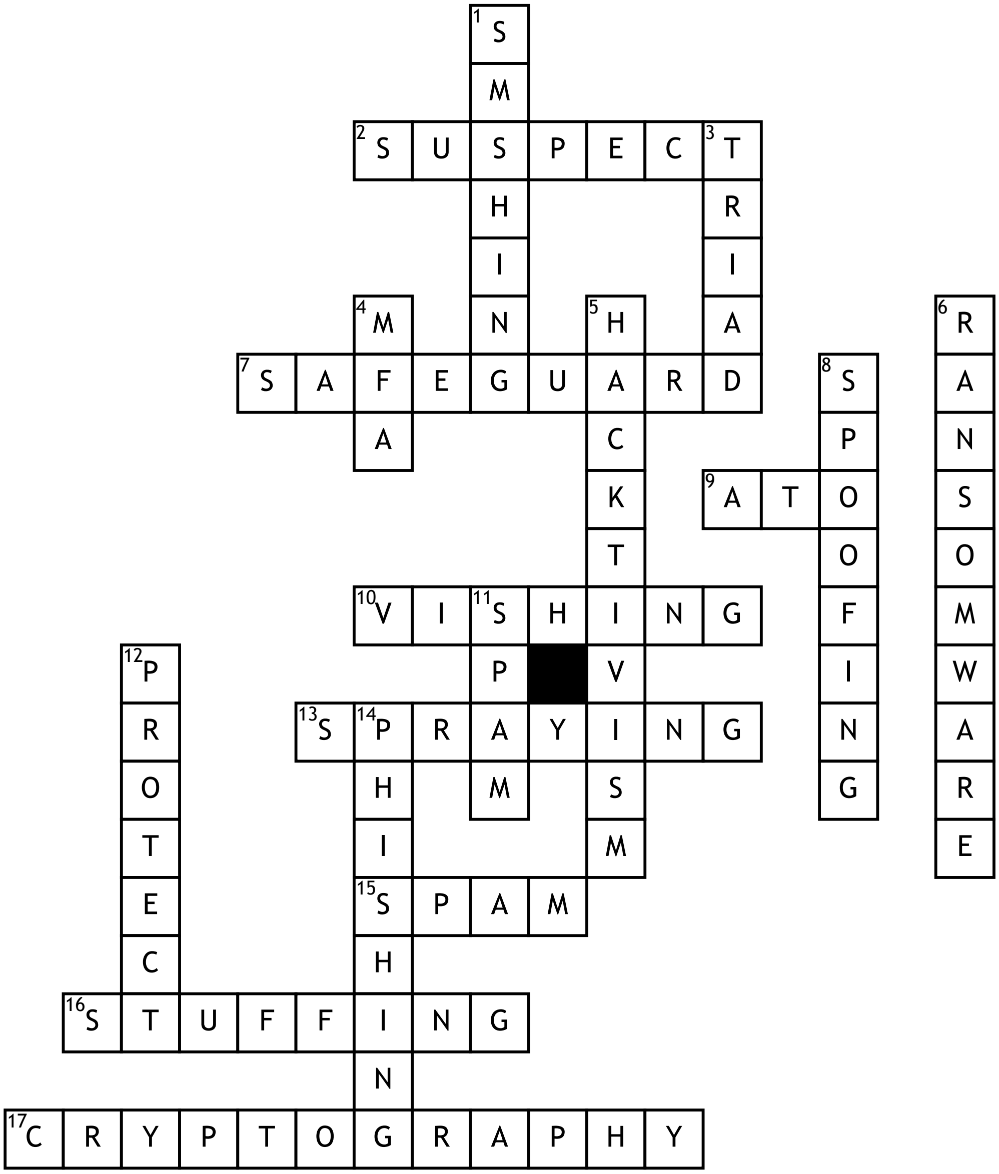
Name: ____ Date: _______

Cybersecurity Basics



Across

2. If you receive a suspicious email that you believe to be a phishing attempt, report it to _______@cfpb..gov

7. Users should take appropriate steps to __________________ their access credentials (i.e. passwords, badges, tokens, etc.) against loss, theft, or unauthorized or improper disclosure.

9. An ______ is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation of a Business Product and explicitly accepts the risk to agency operations.

10. _______is a form of criminal phone fraud, using social engineering over a telephone system to gain access to private, personal, and financial information to steal identities, money, or access.

13. Password ______ is an attack that attempts to access a large number of accounts with a few commonly used passwords.

15. Email __________ is the creation of email messages with a forged sender address.

16. Credential ________________ attacks do not attempt to brute force or guess any passwords - the attacker simply automates the logins for thousands to millions of previously discovered credential pairs using standard web automation tools.

17. Involves creating written or generated codes that allow information to be kept secret.

Down

1. ______ uses cell phone text messages to induce people to divulge their personal information.

3. The CIA _____________ is a model designed to guide policies for information security within an organization. CIA stands for confidentiality, integrity, and availability.

4. ______ or Multi Factor Authentication is an authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.

5. The use of technology to promote a political agenda or a social change.

6. _____________ is a type of malware that threatens to publish data or perpetually block access to it unless a ransom is paid.

8. A ______ is intentional deception made for personal gain or to damage an individual through email.

11. Unauthorized and/or unsolicited electronic mass mailings.

12. Users must physically _______________ CFPB information resources when left unattended. Recommended precations include, but are not limited to, placing sensitive information or devices that contain such information in a locked case, desk drawer, office, or a locked automobile trunk, or securing laptops to a fixed object with a locked cable.

14. _____ is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques.