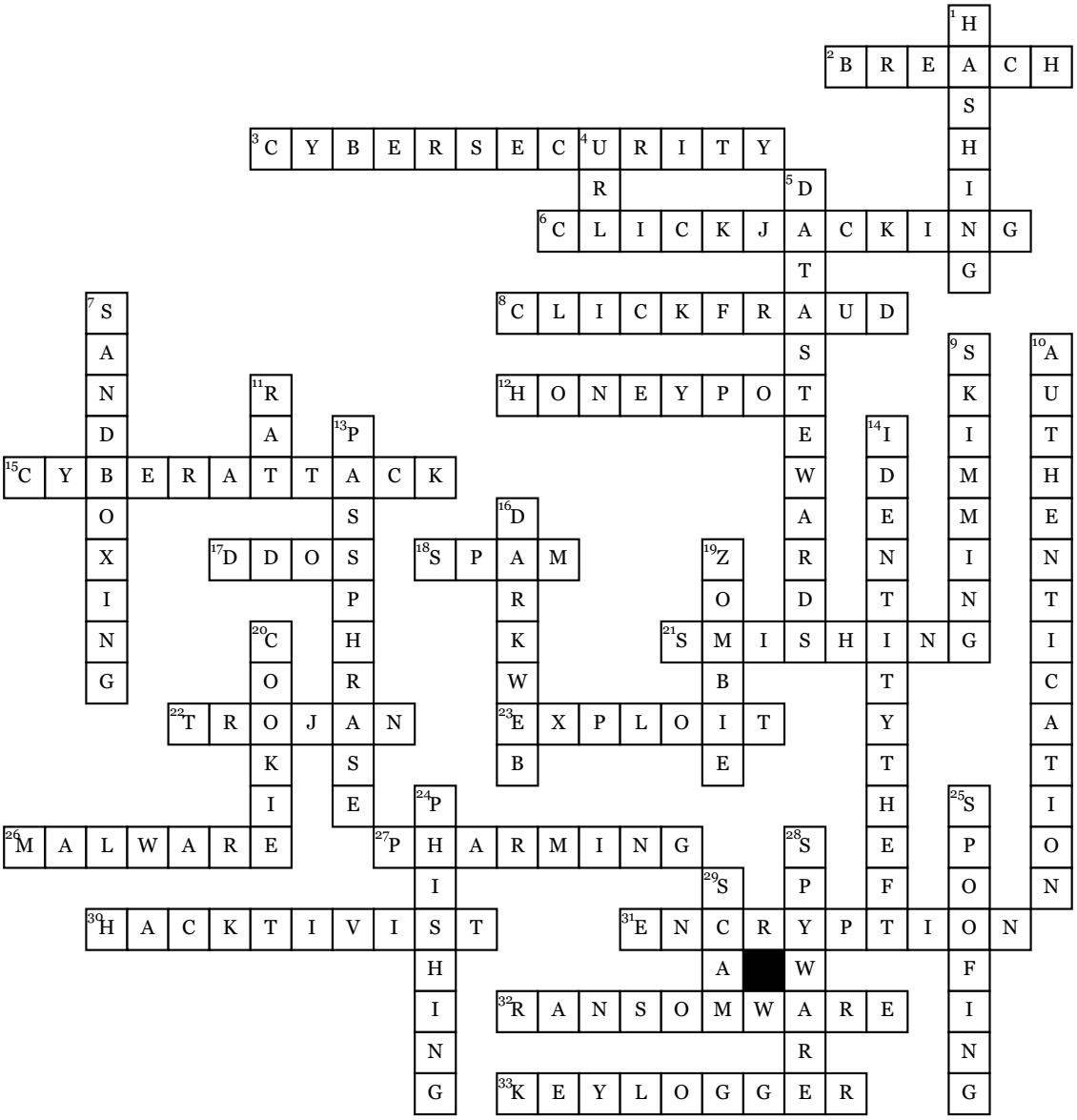
Name: _____ Date: _____

CyberSecurity Awareness 2019



Across

2. The moment a hacker successfully exploits a vulnerability in a computer or device, and gains access to its files and network.
3. The efforts to design, implement, and maintain security for an organization's network, which is connected to the Internet. It is a combination of logical/technical-, physical- and personnel-focused countermeasures, safeguards and security controls.
6. A malicious technique by which a victim is tricked into clicking on a URL, button or other screen object other than that intended by or perceived by the user.
8. This happens when artificially created bogus clicks are used to manipulate Pay-Per-Click (PPC) advertising. The idea behind this practice is to increase the number of payable clicks, in order to generate revenue to advertisers. Cybercrooks use Botnet to create these types of scams.
12. A trap or decoy used to distract attackers in order to prevent them from attacking actual production systems. It is a false system that is configured to look and function as a production system.
15. Any attempt to violate the security perimeter of a logical environment it can focus on gathering information, damaging business processes, exploiting flaws, monitoring targets, interrupting business tasks, extracting value, causing damage to logical or physical assets or using system resources to support attacks against other targets.
17. An acronym that stands for distributed denial of service – a form of cyber attack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).
18. A form of unwanted or unsolicited messages or communications typically received via e-mail but also occurring through text messaging, social networks or VoIP.
21. What is a fraudulent action similar to phishing, using SMS (text) messages rather than e-mail messages to send bait messages to people.
22. malware that appears to perform a benign or useful action but in fact performs a malicious action, such as transmitting a computer virus.
23. A malicious application or script that can be used to take advantage of a computer's vulnerability.
26. a contraction of "malicious software," malware is a general term used to describe software that infiltrates or damages a computer.
27. - The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information
30. An individual who breaches Web sites or secured communications systems to deliver political messages, including those related to foreign policy, or propaganda
31. the process of transforming information to make it unreadable to anyone who doesn't have the password needed to decode it.
32. A form of malware that deliberately prevents you from accessing files on your computer – holding your data hostage. It will typically encrypt files and request that a ransom be paid in order to have them decrypted or recovered.
33. Any means by which the keystrokes of a victim are recorded as they are typed into the physical keyboard. It can be a software solution or a hardware device used to capture anything that is typed on a keyboard

Down

1. A process of applying a mathematical algorithm against a set of data to produce a numeric value (a 'hash value') that represents the data.
4. A Internet address on the World Wide Web. It usually begins with http:// followed by the rest of the name of the resource. It is the common name for a site's web page.
5. Senior officers of the university responsible for determining how data in their area should be handled
7. A means of isolating applications, code or entire operating systems in order to perform testing or evaluation. The sandbox limits the actions and resources available to the constrained item.
9. Skimming is a method used by identity thieves to capture information from a cardholder. Several approaches can be used by fraudsters to procure card information with the most advanced approach involving a small device place at ATMs and other point of sale locations such as a gas station.
10. the process of identifying a piece of information, the veracity of information provided. In computers, it is the process of identifying a person or system with the username; password
11. What is a trojan that stays dormant on a computer until it is remotely activated by another user.
13. a secret phrase that helps protect accounts, files, folders, and other confidential information
14. acquisition and use of a person's private identifying information
16. what is the part of the Internet that is not visible to regular users and is a vast network of websites & portals that are not categorized by search engines.
19. a computer that has been compromised, often by a botnet, so that an unauthorized person has complete control to use the computer to perform malicious tasks.
20. A small text file placed on your computer when you visit a website, that allows the website to keep track of your visit details and store your preferences.
24. Method used by criminals to try to obtain financial or other confidential information (including user names and passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organization
25. 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.
28. Malware that passes information about a computer user's activities to an external party.
29. A term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.