READTHEORY

Name________________
Date________________

• Reading Comprehension 2 Level 11

Directions: *Read the passage. Then answer the questions below.*

The average computer user has between 5 and 15 username/password combinations to log in to email accounts, social networking sites, discussion boards, news and entertainment sites, online stores, online banking accounts, or other websites. For people who use email or other internet applications at work, the number of required username/password combinations may surpass 30. Some of these accounts demand that you use a specific number of symbols and digits, while others require you to change your password every 60 days. When you add to this list the codes needed to access things like ATMs, home alarm systems, padlocks, or voicemail, the number of passwords becomes staggering. The feeling of frustration that results from maintaining a memorized list of login credentials has grown so prevalent that it actually has a name: password fatigue.

Having to remember so many different passwords is irritating, but it can also be dangerous. Because it is virtually impossible to remember a unique password for each of these accounts, many people leave handwritten lists of usernames and passwords on or next to their computers. Others solve this problem by using the same password for every account or using extremely simple passwords. While these practices make it easier to remember login information, they also make it exponentially easier for thieves to hack into accounts.

Single sign-on (SSO) authentication and password management software can help mitigate this problem, but there are drawbacks to both approaches. SSO authentication can be used for related, but independent software systems. With SSO, users log in once to access a variety of different applications. Users only need to remember one password to log in to the main system; the SSO software then automatically logs the user in to other accounts within the system. SSO software is typically used by large companies, schools, or libraries. Password management software, such as KeePass and Password Safe, is most often used on personal computers. These software programs—which have been built into many major web browsers—store passwords in a remote database and automatically “remember” users’ passwords for a variety of sites.

The problem with both SSO authentication and password management software is that the feature that makes them useful is also what makes them vulnerable. If a user loses or forgets the password required to log in to SSO software, the user will then lose access to all of the applications linked to the SSO account. Furthermore, if a hacker can crack the SSO password, he or she will then have access to all of the linked accounts. Users who rely on password management software are susceptible to the same problems, but they also incur the added threat of passwords being compromised because of computer theft.

Although most websites or network systems allow users to recover or change lost passwords by providing email addresses or answering a prompt, this process can waste time and cause further frustration. What is more, recovering a forgotten password is only a temporary solution; it does not address the larger problem of password fatigue.

Some computer scientists have suggested that instead of passwords, computers rely on biometrics. This is a method of recognizing human users based on unique traits, such as fingerprints, voice, or DNA. Biometric identification is currently used by some government agencies and private companies, including the Department of Defense and Disney World. While biometrics would certainly eliminate the need for people to remember passwords, the use of biometrics raises ethical questions concerning privacy and can also be expensive to implement.

The problems associated with SSO, password management software, and biometrics continue to stimulate software engineers and computer security experts to search for the cure to password fatigue. Until they find the perfect solution, however, everyone will simply have to rely on the flawed password system currently in place.

Questions

1) Which of the following best describes the organization of the passage?

A. The passage organizes ideas in order of increasing importance.
B. The author presents an argument and then uses evidence to dismiss opposing views.
C. The author explains a problem, explores solutions, and then dismisses these solutions as inadequate.
D. The author explains a problem and then persuades readers to agree with his or her solution to the problem.
E. The author explains a problem, contextualizes the problem, and ultimately dismisses it as an unnecessary concern.

2) The passage discusses all of the following solutions to password fatigue except

A. writing the passwords down on a piece of paper
B. voice-recognition software
C. KeePass
D. using very simple passwords
E. intelligent encryption

3) As used in paragraph 3, which is the best synonym for **mitigate**?

A. predict
B. postpone
C. investigate
D. lessen
E. complicate

4) According to the passage, SSO authentication software may be safer than password management software because

I. stolen personal computers contain passwords memorized by a user's web browser
II. if a user of password management software forgets his or her login credentials, the user can no longer access any of the applications protected by the password
III. hackers who access password management software can gain access to all of the applications protected by that password

A. I only
B. II only
C. I and II only
D. II and III only
E. I, II, and III

5) Which of the following statements from the passage represents an opinion, as opposed to a fact?

A. "For people who use email or other internet applications at work, the number of required username/password combinations may surpass 30."
B. "The feeling of frustration that results from maintaining a memorized list of login credentials has grown so prevalent that it actually has a name: password fatigue."
C. "Having to remember so many different passwords is irritating, but it can also be dangerous."
D. "Additionally, recovering a forgotten password is only a temporary solution; it does not address the larger problem of password fatigue."
E. "The problems associated with SOS, password management software, and biometrics continue to stimulate software engineers and computer security experts to search for the cure to password fatigue."

6) In paragraph 6, the author notes that “the use of biometrics raises ethical questions concerning privacy.” Which of the following situations could be used as an example to illustrate this point?

A. A thief steals a personal computer with password management software and gains access to private email accounts, credit card numbers, and bank statements.
B. An employee at a company uses a voice recognition system to log in to his computer, only to be called away by his boss. While he is away from the computer but still logged in, another employee snoops on his computer and reads personal email correspondence.
C. A computer hacker gains access to a system that uses SSO software by cracking the password, thus gaining private access to all linked accounts.
D. A company that employs fingerprint identification security software turns over its database of fingerprints to the local police department when a violent crime occurs on its grounds.
E. Even when a person is on password-protected websites, an internet browser tracks the person’s internet use and collects information in order to tailor advertisements to his or her interests.

7) In the final paragraph, the author’s tone can best be described as

A. angry
B. resigned
C. confused
D. hopeful
E. depressed

Answers and Explanations

1) **C**

This passage begins with an explanation of the problem of password fatigue. As the passage progresses, the author discusses multiple different solutions, such as SSO authentication, password management software, and biometrics. For each potential solution, the author identifies the flaws. In the final paragraph, the author dismisses these solutions as insufficient and states that software engineers and computer security experts continue to search for “the perfect solution.” Based on this information, we can describe the organization of the passage this way: the author explains a problem, explores solutions, and then dismisses these solutions as inadequate. Therefore **(C)** is correct. The passage does not contain information to support choices **(A)**, **(B)**, **(D)**, and **(E)**. Therefore they are incorrect.

2) **E**

Intelligent encryption is never mentioned in the passage. Therefore **(E)** is correct. In paragraph 2, the author states that some people who experience password fatigue leave “handwritten lists” next to the computer. This means **(A)** is incorrect. In paragraph 5, the author discusses using biometric identification that can recognize “human users based on unique traits, such as fingerprints, voice, or DNA.” This makes **(B)** incorrect. In paragraph 3, the author mentions password management software and lists KeePass as an example. This means **(C)** is incorrect. In paragraph 2, the author states that some people use “extremely simple passwords.” Therefore **(D)** is incorrect.

3) **D**

mitigate (*verb*): to lessen or alleviate; to make something less harsh, severe, or violent.

In paragraph 3, the author writes, “Single sign-on (SSO) authentication and password management software can help mitigate this problem, but there are drawbacks to both approaches.” Based on this information, we can understand that SSO and password management software are attempts to reduce or lessen the problems of password fatigue, but that they are not perfect. This means *mitigate* means to alleviate or reduce the severity of something, so a good synonym is *lessen*. Therefore **(D)** is correct. *Predict* means to foretell, but SSO and password management software are both proposed solutions to the problem. The software does not predict the problem, but aims to solve it. This makes **(A)** incorrect. *Postpone* means to delay or defer. The software does not delay the problem, but aims to solve it. This means **(B)** is incorrect. *Investigate* means to inquire or explore. The software does not explore the problem, but aims to solve it. Therefore **(C)** is incorrect. *Complicate* means to make something more complex. The software does not make the problem more complex, but aims to solve it. This eliminates **(E)**.

4) **A**

According to the author, those who use password management software (as opposed to SSO) “incur the added threat of passwords being compromised because of computer theft.” This is a heightened threat for users of password management software because it is most commonly used on personal computers, which can easily be stolen; SSO authentication software is “typically used by large companies, schools, or libraries,” which cannot be stolen. In other words, safety concerns associated with personal computer theft are a problem for those who rely on password management software, but not for those who use SSO. This means SSO software may be safer than password management software. This supports **option (I)**. In paragraph 4, the author discusses the flaws in both SSO authentication and password management software. The author states that for both software programs, forgetting a password poses dangers because of the fact that one password grants access to many accounts. Because this is a danger for *both* kinds of software, it does not make SSO safer than password management software. This eliminates **option (II)**. In paragraph 4, the author discusses the flaws in both SSO authentication and password management software. The author states that for both software programs, hackers pose dangers because of the fact that one password grants access to many accounts. Because this is a danger for *both* kinds of software, it does not make SSO safer than password management software. This eliminates **option (III)**. Therefore **(A)** is correct.

5) **C**

A fact is something known to exist or be true as a result of experience or observation. Facts can be proven. An opinion is a belief or judgment that rests on grounds insufficient to produce complete certainty, such as an emotion or personal bias. Opinions cannot be proven true or false. For example, it is a *fact* that roses are flowers, but an *opinion* that roses smell nice. Although most people would be likely to agree with the author’s opinion that having to remember many passwords is irritating, it is still an opinion. Some people might enjoy the challenge of remembering 30 different passwords. Since this statement cannot be proven true, **(C)** is correct. Choices **(A)**, **(B)**, **(D)**, and **(E)** all contain facts based on experience or observation. These statements can be proven. Therefore they are incorrect.

6) **D**

In paragraph 6, the author writes that “the use of biometrics raises ethical questions concerning privacy.” To correctly interpret this question, we must understand the term “biometrics.” Previously in the paragraph, the author defines it as “a method of recognizing human users based on unique traits, such as fingerprints, voice, or DNA.” Based on this information, we can infer that using people’s unique traits, like fingerprints, voice, or DNA, as identification raises ethical questions about privacy because of how the information might be used. A situation that could raise such a concern likely includes a questionable use of these unique, identifying traits. If a company employs fingerprint identification security software and turns its database over to the local police department when a violent crime occurs on its grounds, this could be viewed as a violation of the employees’ privacy. On the other hand, some people may believe that it is ethical to use the database of fingerprints to solve the crime. This situation represents an ethical question concerning privacy and the use of biometrics, so it could be used as an example to illustrate the author’s point. Therefore **(D)** is correct. A thief stealing a personal computer with password management software and gaining access to private information is a privacy concern, but it does not involve the questionable use of biometrics. This means **(A)** is incorrect. Voice-recognition software is an example of biometrics, but an employee snooping on another employee’s computer does not represent an ethical question that is any different than the violation of privacy that occurs from reading someone else’s diary. If the employee’s computer had been password-protected rather than protected by voice recognition, the privacy concern would be the same. This means that the privacy concern is not raised by the use of biometrics, so **(B)** incorrect. SSO software is not a use of biometrics, but a password system, so **(C)** is incorrect. Password-protected websites are not a use of biometrics, so **(E)** is incorrect.

7) **B**

In the final paragraph, the author notes that until a perfect solution is found, “everyone will simply have to rely on the flawed password system currently in place.” The author has accepted the fact that we will have to rely on a flawed system. This means the author’s tone is resigned. Therefore **(B)** is correct. The author does not express anger in the final paragraph, so **(A)** is incorrect. The author does not express confusion in the final paragraph, so **(C)** is incorrect. Although the author discusses the future in the final paragraph, he or she cannot necessarily be described as hopeful that a perfect solution will be found. This means **(D)** is incorrect. Although the author is not necessarily hopeful in the final paragraph, nothing suggests that the author is depressed. This makes **(E)** incorrect.