This is a Class 2 exam

Lebanon Evangelical School
for Boys and Girls
Loueizeh - Baabda

Stage Exam 01
06NOV2023

Do NOT write in this box. Your MARK will be placed here.

Subject :	English
Class :	8C and 8E
Teacher :	Mrs. Maral Malakian Abou Zeid
Duration :	1 hour

Your name :		*Time taken to complete exam*
Your Class :		
Exam Room :		
How many sheets, including cover sheet :		

- Do not open this paper until the teacher in charge instructs you to do so.
- The most important thing to remember in taking an exam is NEVER PANIC.
- If you are caught cheating in this exam, you will be awarded zero for ALL exams that are taken on this day.

VERY IMPROTANT: Do not answer any of the questions on this sheet. Use a separate test block paper to answer on & staple it to the question sheet.

Phishing

Imagine that you get an email one morning. It appears to be from your bank. The email warns that someone broke into your account. It says that you need to sign in to check some things. You click the link in the email. It takes you to a site that looks very much like your bank's. You enter your username and password. You submit the form. You've just been phished!

Phishing is a type of attack that happens over the Internet. Users receive an email or text message that seems like it came from a trusted source. These users are being deceived. They are interacting with dangerous hackers. The attackers copy trusted companies. They send users to web pages that look like the ones we use everyday. When users login or provide sensitive information, the attackers steal this data.

Attackers want your data for many reasons. They may use your data to commit identity fraud. This is when they use your identity to buy something with your credit. Then they receive the goods and you receive the bill. Or they may want your password to take over a computer network. They may want access to private emails. They may want customer records. They gain access by tricking people into giving them their login info.

Some phishing attacks are targeted. A targeted phishing attack is called a spear phishing attack. These attacks are dangerous because they are convincing. The attacker may know the target's name, address, or job title. They may have gathered info from social networks, like the names of friends or family. The attackers may use this personal information to craft a believable email. The target will be tricked into clicking a link. The link will send them to a phony website. This site will look familiar, but it will be a spoofed site built to steal data. Any data that the target submits will go to the hacker.

Phishing attacks are dangerous, but you can spot them if you pay attention. One thing to watch is your address bar in your browser. Attackers use domains that look like the ones that we trust, but they are not the same. For example, in 2016 staffers from Hillary Clinton's campaign were spear phished. The attackers used the domain accounts-google.com. That domain looks like google.com, but it isn't the same. When logging into google, you should always do it from google.com. Likewise, when logging into any account, make sure the address matches what you expect. If you are unsure, search for the site and login from the root domain.

An even better way to secure your account against phishing attacks is to use 2FA: two factor authentication. 2FA means that your account is secured with two keys. The first is your password. The second key is a random code that changes every few minutes. This code may be generated by a 2FA app, like Authy. Or it can be sent to your cell phone on request. If you activate 2FA on your accounts, an attacker will not be able to get in even with your password.

Phishing attacks are scary and common. The reason why they are common is that they are effective. Many people accept appearances without suspicion. Browsing the Internet safely requires a healthy amount of suspicion. Not everything is what it appears. Nobody is trying to give you free money. Don't trust; verify.

A. Circle the correct answer: (10pts. 2 pts. each)

1. Which is a phishing attack?
   a) Throwing water on an adversary's computer.
   b) Tricking someone into giving away sensitive data.
   c) Sneaking into a concert without paying.
   d) Buying something with someone else's credit.

2. Which statement would the author most likely AGREE with?
   a) Every phishing attack involves stealing the victim's identity to commit fraud.
   b) In a phishing attack, an attacker overpowers a victim with a stronger computer.
   c) In a spear phishing attack, the attacker erases the victim's identity.
   d) If a phishing attack is successful, users willingly give attackers sensitive data.

3. How can 2FA protect users from phishing attacks?
   a) Nobody can log into the account under any circumstances.
   b) The attacker needs a fingerprint or eyeball scan to access the account.
   c) Users need two keys to login, and the user can't give away one of the keys.
   d) Two people have to approve the login, so the attacker can't do it alone.

4. What is the difference between a phishing and spear phishing attack?
   a) A spear phishing attack is targeted while phishing is random.
   b) A phishing attack is illegal while spear phishing is legal.
   c) A spear phishing attack involves theft or identity fraud and phishing does not.
   d) A phishing attack is more convincing than a spear phishing attack.

5. Why does the author discuss 2FA?
   a) He is trying to impress readers by using technical terms.
   b) He is trying to persuade readers to not use the Internet.
   c) He is trying to inform readers about how to protect themselves.
   d) He is trying to entertain readers by telling a short story.

B. Comprehension Questions: (10pts. 5 pts. each)

1. Which is more dangerous a phishing or a spear phishing attack? Explain why or why not by supporting it with examples from the text?

2. In your own words, explain what 2FA is, and how it protects users against phishing attacks?

C. Grammar Exercises

Complete the sentences with the present simple or present continuous forms of the verbs in brackets. (10pts. 2 pts. each)

1) These days, most children (have) too much fizzy drinks.
2) You (take) any vitamins at the moment?
3) We (not go) to Chinese restaurants very often.
4) What your mother (make)? It smells great!
5) He (want) to become a doctor in the future.

Put the verbs in brackets in the correct form (present simple or present continuous). (20pts., 2 pts. each)

Next week, my friends and I (go) camping in the woods. I (prepare) the food, because I (like) cooking. Dave (have) a big car with a trailer, so he (provide) the transportation. Sam (bring) the tent, he (go) camping every year. My wife (think) we're crazy. She (spend) holidays in comfortable hotels, so right now she (take) a trip to Paris instead.

Maral Malakian Abou Zeid

SE01 Answer Key

8C – 8E

A. (10 pts. 2 pts. each)

1) b
2) d
3) c
4) a
5) c

B. (10 pts. 5 pts. each)

1) Phishing attacks are not as dangerous as spear phishing attacks. Since, spear phishing is targeted and convincing and can't be easily caught. This is precisely where the attacker will examine your personal social networks for personal data about you. He will then take advantage of this to deceive the target by using well known emails or bogus websites. As a result, the hacker will receive all of the data we supply. Traditional phishing, however, is more easily identified. Given that, attackers use domains that resemble the ones we are familiar with, but they are not identical. In this scenario, we must monitor our browser's address bar.

2) A security feature known as two factor authentication, or 2FA, demands two distinct forms of identity in order to access our accounts. A password is the first key, and most of the time, a code that is sent to our smartphones is included in the second. In order to prevent the attacker from hacking us, we should enable 2FA on our accounts.

C. (10 pts. 2 pts. each)

1) are having
2) Are you taking
3) don't go
4) is your mother making
5) wants

(20 pts. 2pts. each)

are going - am preparing – like – has – is providing - is bringing – goes – thinks – spends – is taking