Name: _____

Nonfiction Reading Test
Phishing

Directions: Read the following passage and answer the questions that follow. Refer to the text to check your answers when appropriate.

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 hey 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.

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. 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.

3. Which is NOT a motive or reason for phishing mentioned in the text?

a) To steal private communication or records
b) To commit identity fraud
c) To gain control of someone else's computer network
d) To disarm home alarm systems

4. 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.

5. 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.

6. Which statement would the author most likely DISAGREE with?

a) Hilary Clinton's campaign team was spear phished in 2016.
b) The domains google.com and accounts-google.com go to the same place.
c) Some links send users to phony sites designed to steal passwords.
d) You should check your address bar carefully before submitting your data.

7. Which best describes the main idea of the third paragraph?

a) To describe the reasons for phishing attacks
b) To explain how phishing attacks are executed
c) To teach readers how to defend against phishing attacks
d) To compare and contrast phishing and spear phishing

8. 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.

9. Which is NOT discussed by the author?

a) Reasons why people commit phishing attacks
b) Which computers work best for phishing attacks
c) How spear phishing is different from phishing
d) How to protect oneself against phishing attacks

10. With which statement would the author most likely AGREE?

a) A safe Internet user is suspicious of links.
b) A company's logo on a web page means that the site is safe.
c) Using 2FA does NOT help to protect against phishing attacks.
d) The Internet is too dangerous for regular people to use.

1. Explain in your own words what 2FA is and how it protects users against phishing attacks.

2. What is the difference between a phishing and spear phishing attack? Which is more dangerous and why do you think that?