

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 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.

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.

Name: _____

Nonfiction Reading Test

Y2K

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

The year was 1999. The night was December 31st, New Year's Eve. The world watched and waited. It was a night of celebration. But it was also a night of fear. People had grown to depend on computers. Computers powered our banks. They ran our companies. Would they all break at midnight? Some thought that they might. But why?

The Year 2000 problem, or Y2K, had to do with computer storage. Computers store data and files in memory. Computer memory is cheap these days. Some companies will give you cloud storage for free. But in the early days of computing, memory was very expensive. One kilobyte (about 1,000 characters of storage) might cost as much as \$100 USD.

People had to think of ways to use less storage. One way they did this was by storing only the last two digits of the year. Instead of saving the date as 07/02/1979, they would save it as 07/02/79.

This seemed like a good idea at first. But as the years passed, the turn of the century neared. Would our computers know that it was the year 2000 instead of the year 1900? How could they? What would happen if they got the dates wrong? Would the computers break?

The Y2K problem worried many people. Some feared that banking systems wouldn't work. Payments might fail. Cash registers might break.



Another fear was that transportation systems would break. Taxi meters could stop working. Airline computers could fail. Traffic lights could shut down. The Y2K problem was very worrisome.

But people didn't just wait for their systems to fail. They worked hard to prevent the bugs. Governments passed laws. Businesses upgraded their systems. People rewrote software. Some think over \$300 billion dollars were spent fixing the Y2K problem. But were people really prepared when it happened?

As clocks turned and calendars flipped to the year 2000, there were very few problems. Air planes did not fall from the sky. Power grids did not shut down. Bank accounts did not get wiped out. We had avoided the worst.

A few bugs and errors happened around the world. Some bus ticket machines in Australia stopped working. Some slot machines in Delaware broke. Certain cell phones in Japan deleted new text messages. But most computers kept working just fine. Will things work out the same way for the Year 2038 problem (Y2K38)? Only time will tell.

Name: _____

Y2K (Questions)

1. Which best describes the Y2K problem?
 - a) Magnetic waves might erase all computer memory.
 - b) Computers would cost too much for most families.
 - c) A computer virus would spread and break all systems.
 - d) Computers might get the date wrong and malfunction.

2. Which best explains why programmers shortened dates in computer storage?
 - a) They were in a big hurry.
 - b) They were trying to save money.
 - c) They were being lazy.
 - d) They were creating more work for themselves.

3. Which best describes the author's purpose in writing the SIXTH paragraph?
 - a) He is describing fears related to transportation and the Y2K bug.
 - b) He is informing readers of how computers help people.
 - c) He is explaining how a terrorist attack affected America on 9/11.
 - d) He is persuading readers to back up their computer storage.

4. Which is NOT a way that people addressed the Y2K problem according to the text?
 - a) Programmers rewrote software.
 - b) Companies upgraded their computer systems.
 - c) Individuals threw away outdated computers.
 - d) Governments created legislation.

5. Which best describes the TEXT STRUCTURE in the THIRD paragraph?
 - a) Problem and solution
 - b) Order of importance
 - c) Chronological order
 - d) Spatial order

6. Which of the following was NOT listed in the text as a fear related to Y2K?
 - a) Traffic control devices would fail.
 - b) School bells would not ring on time.
 - c) Bank systems would malfunction.
 - d) Airline computers would stop working.

7. Which best describes HOW the Y2K bug affected the world?

- a) Many computers malfunctioned and it was a catastrophe.
- b) All computers stopped working and the damage was tremendous.
- c) A small number of computers malfunctioned but it was no big deal.
- d) Most computers stopped working and it cost a lot of money.

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

- a) It was a tragedy that people did not prepare more for Y2K.
- b) Y2K was never a problem and people were worried for no reason.
- c) Computers create more problems than they solve.
- d) Since people prepared for Y2K, it wasn't much of a problem.

9. Which was NOT an error caused by the Y2K bug?

- a) Credit card processors around the world went down.
- b) Bus ticket machines in Australia stopped working.
- c) Cell phones in Japan deleted new messages.
- d) Slot machines in Delaware malfunctioned.

10. What lesson can readers learn from this text?

- a) Technology is frustrating and not worth having.
- b) Our dependence on technology can be scary at times.
- c) Robots and AI will take over the world one day.
- d) Y2K was the worst catastrophe in history.

1. In your own words, explain the Y2K problem. Then describe how people responded to the Y2K problem. Do you think that their response was successful? Why or why not? Refer to the text in your answer.

2. Are we *too* dependent on technology as a society? Quote text to support your position. Explain the text you quoted and how it relates to your argument.

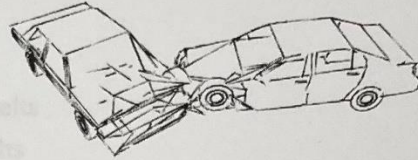
Name: _____

Nonfiction Reading Test

Seat Belts

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

"Click!" That's the sound of safety. That's the sound of survival. That's the sound of a seat belt locking in place. Seat belts save lives and that's a fact. That's why I don't drive anywhere until mine is on tight. Choosing to wear your seat belt is as simple as choosing between life and death. Which one do you choose?



Think about it. When you're driving in a car, you may be going 60 MPH or faster. That car is zipping down the road. Then somebody ahead of you locks up his or her brakes. Your driver doesn't have time to stop. The car that you are in crashes. Your car was going 60 miles per hour. Now it has suddenly stopped. Your body, however, is still going 60 MPH. What's going to stop your body? Will it be the windshield or your seat belt? Every time that you get into a car you make that choice. I choose the seat belt.

Some people think that seat belts are uncool. They think that seat belts cramp their style, or that seat belts are uncomfortable. To them I say, what's more uncomfortable? Wearing a seat belt or flying through a car windshield? What's more uncool? Being safely anchored to a car, or skidding across the road in your jean shorts? Wearing a seat belt is both cooler and more comfortable than the **alternatives**.

Let's just take a closer look at your choices. If you are not wearing your seat belt, you can hop around the car and slide in and out of your seat easily. That sounds like a lot of fun. But, you are also more likely to die or suffer serious injuries. If you are wearing a seat belt, you have to stay in your seat. That's no fun. But, you are much more likely to walk away unharmed from a car accident. Hmmm... A small pleasure for a serious pain. That's a tough choice. I think that I'll avoid the serious pain.

How about giving money away? Do you like to give your money away? Probably not. And when you don't wear your seat belt, you are begging to give your money away. That's because kids are required to wear seat belts in every state in America. If you're riding in a car, and you don't have a seat belt on, the police can give you or your driver a ticket. Then you will have to give money to the city. I'd rather keep my money, but you can spend yours how you want.

Wearing a seat belt does not make you **invincible**. You can still get hurt or killed while wearing your seat belt. But wearing them has proven to be safer than driving without them. You are much less likely to be killed in a car wreck if you are wearing a seat belt. You are much less likely to get seriously injured if you are wearing one. So why not take the safer way? Why not go the way that has been proven to result in fewer deaths? You do want to live, don't you?

1. Which title best expresses the main idea of this text?

- a. *Car Accidents: Ways That We Can Prevent Them*
- b. *Slow Down: Save Lives By Driving Slower*
- c. *Seat Belts: Wear Them to Survive Any Wreck*
- d. *Why Not? Improve Your Odds with Seat Belts*

2. Which best expresses the author's main purpose in writing this text?

- a. To inform readers about seat belt laws
- b. To persuade readers to wear seat belts
- c. To entertain readers with stories and jokes about seat belts
- d. To describe what car accidents are like without seat belts

3. Which best describes the text structure in the fourth paragraph?

- a. Compare and contrast
- b. Chronological order
- c. Sequential order
- d. Problem and solution

4. Which best defines the word *alternatives* as it is used in the third paragraph?

- a. Being safe
- b. Being unsafe
- c. Other choices
- d. Driving fast

5. Which best expresses the main idea of the fifth paragraph?

- a. Seat belts are a waste of money.
- b. People don't like to give money away.
- c. Not wearing a seat belt may cost you.
- d. Seat belt laws save lives.

6. Which best defines the word *invincible* as it is used in the last paragraph?

- a. Uncool
- b. Difficult or impossible to see
- c. Glow-in-the-dark
- d. Unable to be harmed

7. Which statement would the author most likely **agree** with?

- a. Being safe is more important than being cool.
- b. Moving freely around a car is worth the risks.
- c. Seat belts will keep you safe in any car accident.
- d. You should be most concerned with your comfort.

8. Which argument is **not** made by the author?

- a. Not wearing a seat belt can be expensive.
- b. Penalties for not wearing a seat belt should increase.
- c. Seat belts keep you from flying through the windshield.
- d. Wearing a seat belt is cooler than suffering an injury.

