Name _____ Date _____

Phishing and Online Scams: Spot the Warning Signs

Directions: Each question describes something a student runs into online: a message, a link, a web page or a pop-up. Read each one closely before you answer.

1. Zara is playing a game called Moonbolt when another player, who says he is a game moderator, sends her a chat message: "Send me your password so I can check your account, or you will be banned today." What should Zara do first?

A. Send the password, because moderators help run the game.

B. Keep her password private and show the chat to a trusted adult.

C. Ask him to prove he is a moderator before she sends it.

D. Send the password, then change it once he is done checking.

2. Priya plays a game called Glimmerdeep, and one day she gets this email:

"Hi Priya! This is Glimmerdeep Support. We noticed that someone tried to sign in to your account from a new device. Tap the link below and enter your password within one hour, or your account and all of your saved worlds will be deleted. Thanks for playing Glimmerdeep!"

Which details are warning signs of phishing? Choose 3.

☐ A. It greets Priya by her first name.

☐ B. It names a game Priya really plays.

☐ C. It gives her only one hour to act.

☐ D. It says her account and saved worlds will be deleted.

☐ E. It asks her to enter her password through a link.

☐ F. It thanks her for playing.

3. Diego's school library website is bookwhistle.org, and he gets an email asking him to sign in and renew his library books. Which web address is a fake made to look like the real site? Look closely at each one.

A. bookwhistle.org

B. bookwhistle.org/sign-in

C. bookwhist1e.org/sign-in

D. bookwhistle.org/help

4. Mei taps a link in a text message and lands on a page that asks for her Chatterbloom password. Next to the web address, she notices a small padlock icon. What does the padlock tell her?

A. Someone has checked the page and found that it is safe.

B. The page belongs to the real Chatterbloom company.

C. Her password will stay secret from whoever runs the page.

D. Her connection to the page is encrypted, but the page itself could still be a fake.

5. Ayla gets a text that seems to come from her video app, Flickberry, saying there is a problem with her account. She shows the text to her mom, and together they want to find out whether the problem is real. What is the safest way for them to check?

A. Open the Flickberry app the usual way, not through the text, and look at her account.

B. Call the phone number listed in the text.

C. Reply to the text and ask for proof that it is real.

D. Tap the link in the text, but don't type anything on the page.

6. Ben gets a message from his friend Omar's account that says, "Is this you in this video?" and includes a link. Omar never sends messages like this. What is the best first step for Ben?

A. Leave the link alone and ask Omar another way, like in person or by phone, if he sent it.

B. Send the link to a few friends to see if it works for them.

C. Reply in the same chat and ask Omar if the link is safe.

D. Tap the link quickly to see what the video shows.

7. Each message below came from a scammer. Match each message to what the scammer is trying to get.

Write the letter of the matching answer on each line.

1. _____ "There is a problem with your account. Type your password at this link to fix it."
2. _____ "Our driver can't find your house. Reply with your street address."
3. _____ "Your teacher sent you a file. Open the attachment and install the program to see your grade."
4. _____ "We just texted you a 6-digit code. Send it back to us to confirm your account."

Choices for question 7

A. The code that keeps others out of your account

B. A way to put harmful software on your device

C. Your home address

D. Your password

8. Hana typed her Lumigrove password into a page she reached from a link in a text message, and then she noticed that the web address was misspelled. She told her dad right away, and he is sitting with her now. What should they do next?

A. Wait a few days to see if anything strange happens to her account.

B. Go back to the fake page and sign out of it.

C. Go to the real Lumigrove app and change her password, plus any other account that uses the same one.

D. Delete the text so the scammer can't use her password.

9. Lucia gets a text from a number she doesn't recognize: "You won a free tablet! Reply with your full name and school to claim it." Her aunt reads the message with her, and they both agree it is a scam. Lucia has not replied yet. What should she do with the text?

A. Reply to tell the sender she knows it is a scam.

B. Keep it in case the prize turns out to be real.

C. Reply with a made-up name to trick the scammer.

D. Report it as junk or spam on her phone, then delete it.

10. Nora is playing on a game website when a pop-up suddenly fills her tablet screen. It flashes red and says, "Virus found! Tap Clean Now right away!" What is the safest first move for Nora?

A. Type her password into the pop-up so it can start a scan.

B. Tap Clean Now so the virus is removed quickly.

C. Tap the pop-up's message to read more about the virus.

D. Close the browser tab without tapping anything inside the pop-up.