

Spot the phish



Grades: 6 to 9

Phishing messages are designed to trick people into clicking a link, sharing information or taking action quickly. They can appear in texts, emails, direct messages or even messages that seem to come from someone you know.

In this activity, you'll look for clues that a message may be fake. Circle Real or Fake for each example and explain what helped you decide. In real life, if you're unsure, verify the message another way before clicking or replying.

Part 1

Real or fake?

Read each message. Circle Real or Fake, then underline or write down the clue that helped you decide.

- 1. Your school library account: "The book you placed on hold is ready for pickup. Sign in through the school library website to view your account."**

Real Fake

Clue: _____

- 2. An email in your inbox: "URGENT! Your account will be deleted TODAY. Click <http://account-check.example> to keep access. Enter your password to confirm."**

Real Fake

Clue: _____

- 3. A message from your classmate: “Hey, is this you in this video??” followed by a shortened link, even though you weren’t expecting a message from them.**

Real Fake

Clue: _____

- 4. Your teacher’s post in the class learning platform: “Reminder: tomorrow’s assignment is due at 3 p.m. You can find the instructions in our class folder.”**

Real Fake

Clue: _____

- 5. A text message on your phone: “Congratulations! You have been selected for a free phone. Reply with your full name, address and birth date to claim it.”**

Real Fake

Clue: _____

Part 2:

Phishing clue check

Which clues can be signs of phishing? Put a check beside every clue that could make you stop and look more closely.

- The message pressures you to act immediately
- The sender or address looks unfamiliar or slightly different than expected
- The message asks for a password, payment or personal information
- The link looks unusual, misspelled, shortened or unrelated to the sender
- The message promises a prize or offer that seems too good to be true
- The message arrives through a channel you normally use

Remember: No single clue proves a message is phishing. Look at the whole situation, and verify through a trusted source when you are unsure.

Part 3:

Reflection

1. You receive a suspicious message from a friend's account. What could you do before clicking anything?

2. What is one way you can verify whether a message is legitimate?
