COMPUTING AND DIGITAL LITERACY

Phishing and Scams

Difficulty level: Easy

Computing and Digital Literacy

This document was made by AI and there may be mistakes. If a question or answer looks wrong, use the Flag a mistake button to let Brett know so he can fix it.

Overview of the concept

This is how you spot a fake message pretending to be your bank or a delivery company before you click a link or hand over your password. A scammer sends a message that looks urgent, like your account is locked or your parcel is stuck, because urgency makes people click before they think. The giveaways are usually small, like a strange sender address, a link that does not match the company, or a message asking for a password a real bank would never ask for. Stopping to check the sender before you click is the habit that keeps your money and your accounts safe.



© 2026 Brett Robbins. All Rights Reserved.

Rule

Phishing: a phishing message pretends to be from a company you trust, uses urgency to make you click, and asks for a password, a fee, or bank details.

Check the sender address letter by letter for lookalike spellings, such as a zero for the letter o. Ask whether you entered anything or expected the message. Real prizes never ask for a fee, and real companies never ask for your password by message. Do not click: go to the real site yourself.

© 2026 Brett Robbins. All Rights Reserved.

Worked examples

EXAMPLE 1

Q **An email arrives from support@amaz0n-help.com, with the subject 'URGENT: verify now or lose your account!', and a link to a strange address. Is it phishing, and what should you do?**

Inbox

From: support@amaz0n-help.com

Subject: URGENT: verify now or lose your account!

Dear customer,

Your account will be closed. Verify now:

https://amaz0n-help.com/verify

Thank you, Support Team

SOLUTION

From: support@amaz0n-help.com (note the 0)

Subject: URGENT: verify now or lose your account!

Link goes to a strange address, not amazon.com.

Look at the sender address one letter at a time and watch for spellings that only look right.

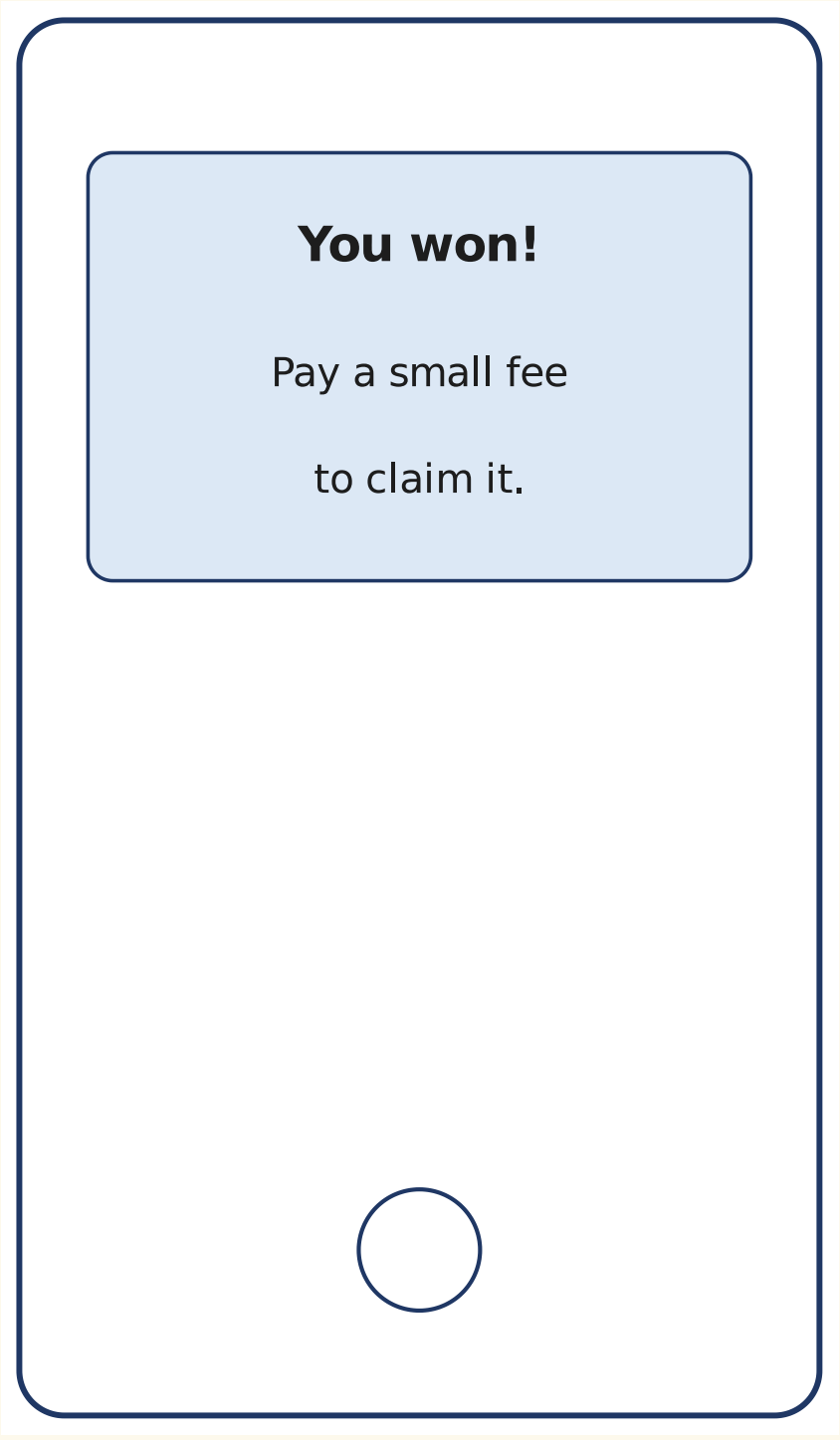
Notice the pressure: urgent threats are a classic scam tactic.

Do not click. Go to the real site yourself by typing its address, or contact the company another way.

© 2026 Brett Robbins. All Rights Reserved.

EXAMPLE 2

Q You get a message saying 'You won! Pay a small fee to claim it,' but you never entered a contest. What should you do?



SOLUTION

© 2026 Brett Robbins. All Rights Reserved.

Message: 'You won! Pay a small fee to claim it.'

Check: you never entered a contest.

Action: delete it and report it; real prizes do not ask for fees.

Ask yourself whether you typed anything in, or were expecting a message like this.

Remember that real prizes do not demand a fee, gift cards, or bank details to claim.

Delete the message and report it using the report button or your provider's scam report.

© 2026 Brett Robbins. All Rights Reserved.

Practice questions

1 **Read this email: From: support@amaz0n-help.com. Subject: URGENT: verify now or lose your account! The link goes to a strange address. Which two signs show it is phishing?**

- **A** The email has a company logo, and the urgent threat pressures you to act.
- **B** The sender address uses a 0 instead of an o, and the urgent threat pressures you to act.
- **C** The sender address uses a 0 instead of an o, and the email arrived on a weekday.
- **D** The sender address uses a 0 instead of an o, and the email wishes you a good day.

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

2

Read this email: From: bank@secure-paypal.net. Subject: Your account will close today! Click here. The link goes to paypal-secure-login.net, not paypal.com. What does the link tell you?

A. The link does not match the real company, so the email is phishing.

B. The link proves the email is genuine because it mentions PayPal.

C. The link means the email arrived quickly.

D. The link shows the email was sent on a weekday.

Understand It with Pulse

Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

3

What should you check first in a suspicious email?

A The sender's real address, letter by letter

B The company logo

C How quickly the email arrived

D The day of the week it arrived

Understand It with Pulse

Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

4 A message has a familiar logo but a strange sender address. Is it genuine?

- **A** Probably not: logos are easy to copy, so check the sender address.
- **B** Yes: a familiar logo proves it is genuine.
- **C** Probably not: the message arrived too quickly.
- **D** Yes: a strange sender address is normal.

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

5

A message from a friend's account says they are stuck abroad and asks you to send a gift card code right away. You were not expecting this. What should you do?

- **A** Do not send a code; contact your friend another way to check
- **B** Send the code, then ask your friend about it later
- **C** Reply with your own bank details so they know it is you
- **D** Forward the message to all your contacts

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

6

You get a message: 'You won a phone! Pay $10 to claim it.' You never entered a contest. What should you do?

- A Do not pay; delete it and report it.
- B Pay the $10, then report it
- C Send your bank details to claim it faster
- D Reply asking for a bigger prize

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

7

You get a message: 'You won $500! Send your bank details to claim it.' What should you do?

A Do not send bank details; delete it and report it.

B Send your bank details, then delete the message

C Pay a small fee to claim the prize

D Forward the message to your friends

Understand It with Pulse

Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

8

Why do real prizes never ask for a fee to claim them?

A Because real prizes are always small.

B Because a fee makes the prize arrive faster.

C Because a real prize is already yours; a fee is how the scam takes your money.

D Because real prizes are only won online.

Understand It with Pulse

Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

9 What is phishing?

- **A** A fake message pretending to be a trusted company to steal details
- **B** A real message from your bank
- **C** A way to win prizes online
- **D** A kind of computer virus that deletes your files

Understand It with Pulse | Flag a mistake

10 Why do scammers use urgent language?

- **A** To rush you into acting before you check
- **B** To make the message look friendly
- **C** To help you read it faster
- **D** To prove the message is genuine

Understand It with Pulse | Flag a mistake

© 2026 Brett Robbins. All Rights Reserved.

ANSWER KEY

1. The sender address uses a 0 instead of an o, and the urgent threat pressures you to act.
2. The link does not match the real company, so the email is phishing.
3. The sender's real address, letter by letter
4. Probably not: logos are easy to copy, so check the sender address.
5. Do not send a code; contact your friend another way to check
6. Do not pay; delete it and report it.
7. Do not send bank details; delete it and report it.
8. Because a real prize is already yours; a fee is how the scam takes your money.
9. A fake message pretending to be a trusted company to steal details
10. To rush you into acting before you check

© 2026 Brett Robbins. All Rights Reserved.