FREE PRACTICE | NEXTGEN

# Digital Money Safety Check

Cleo the Promise Keeper protects information as carefully as money. A scam may imitate a school, bank, game, or friend. A familiar logo is not proof. Check through a known official app, website, or telephone number instead of following instructions in an unexpected message.

## Worked example: a fictional prize message

> **'Congratulations! You won a console. In the next 10 minutes, send us a gift-card code and your account password to unlock it.'**

Warning signs are a surprise prize, a rushed deadline, an unusual payment demand, and a request for a password. Stop interacting, show a trusted adult, and verify independently. Do not send money or a code to test whether the message is real.

## Choose a safe next step

1. A message says a school lunch account is frozen and provides a shortened link. You were not expecting it. What do you do first?

2. An online teammate asks for a one-time login code to 'keep your account safe.' Explain why you should not share it.

3. A pretend shop offers a huge discount but only accepts payment by gift-card codes. Name two warning signs.

All messages here are invented. Do not enter real passwords, card numbers, contact details, or account information into practice activities.

© 2026 Penny Hollow. Educational use under the included license.

DIGITAL MONEY SAFETY CHECK

# Check, explain, and apply

## Model safe responses

1. Open the school's known official website or app with an adult, or contact the office using a trusted number. Do not use the unexpected link or reply with account details.

2. A one-time code can unlock an account. Someone claiming to help may be trying to sign in as you. Keep the code private and contact the service through its official channel if worried.

3. An unusually large bargain plus payment only by gift-card codes is a strong warning. A real-looking page alone does not establish trust.

## Build a safety routine

- Use a different strong password for each account; a trusted adult can help set up a reputable password manager.

- Use multifactor authentication when available. Never approve an unexpected sign-in request or share a verification code.

- If you clicked or shared something, tell a trusted adult quickly. Use official account recovery channels, change exposed credentials, and ask the provider about unauthorized activity.

## Make a reminder

1. Write a three-step 'Pause, verify, protect' rule that you could keep near a device. Include one trusted adult or official route without recording private contact details.

Sources: consumer.ftc.gov/articles/how-recognize-avoid-phishing-scams ; consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts .

Free print license: households and educators may copy this unchanged resource for their own learners. Do not sell, upload as a paid product, or remove Penny Hollow attribution. Keep all practice details fictional; no personal financial information is needed.

© 2026 Penny Hollow. Educational use under the included license.