

CLASSROOM LESSON · GRADES 6-8

# Spot the scam

Free currency, fake giveaways and code requests in game chat, DMs and texts

Students learn the four most common scam hooks aimed at gamers and phone users their age (free currency, 'verify your account' threats, fake giveaways and one-time code requests), hunt for red flags in printed mock messages, sort them into Scam, Probably fine or Check first, and practice the report, block and tell-an-adult routine.



GRADE BAND  
**6-8**

TIME  
**45 minutes**

FORMAT  
**Whole class + groups**

PREP  
**Print & cut, ~10 min**

**BIG IDEA**



**Scams run on hurry and on something free; when a message rushes you or asks for a login or code, stop, check another way and tell someone.**



**Students will be able to**

- ☐ Name four common scam hooks in game chat, DMs and texts: free currency, 'verify your account' threats, fake giveaways and requests for a one-time code
- ☐ Find at least three red flags in a mock message, such as a countdown, a lookalike link or a request for a password or code
- ☐ Sort messages into Scam, Probably fine or Check first and explain the reasoning
- ☐ Describe the report, block and tell-an-adult routine, and how to check a message by going to the app or a known contact directly



**Materials**

- Projector or board for the slide outline
- Worksheet 1: Scam, Probably fine or Check first (1 per student; contains 12 printed mock messages)
- Worksheet 2: Scam-spotter crossword (1 per student, for early finishers or homework)
- Scenario cards (1 set per group of 3-4, cut apart)
- Two colors of highlighter or pen per group, for marking red flags
- Sticky notes or half sheets for the exit ticket

**Before class**

- Print Worksheet 1 single-sided so groups can cut the 12 messages into strips if you want a hands-on sort. Print Worksheet 2 and the scenario cards.
- Label three areas of the board: Scam, Probably fine, Check first.
- Write on the board who students can tell at school (a teacher, the school counselor, the front office) and how to reach your district help desk if a school account is involved.
- Read the answer key for Worksheet 1. The Check first items are the most important discussion points.



**Vocabulary**

- **Scam** — A trick to get your money, your account, your personal information or your items.
- **Phishing** — A fake message that pretends to be from someone you trust to get you to click a link, log in on a fake page or share information. In texts it is sometimes called smishing.
- **One-time code (verification code)** — A short code sent to your phone, email or app to prove it is really you logging in. It is for you only. Anyone who asks for it is trying to get into your account.
- **Red flag** — A clue that something is wrong, such as a countdown timer, a misspelled sender or a link that does not match the real website.

## **Vocabulary** (continued)

- **Lookalike link** — A web address made to look like a real one, with extra words, swapped letters or a different ending, so you think it is the real site.
- **Report and block** — Tools in apps and games that tell the platform about a scammer and stop that account from contacting you again.
- **Account takeover** — When someone else gets into your account and uses it, often to trade away your items or to scam your friends.

## **Standards alignment**

- **ISTE Standards for Students 1.2.d** — Digital privacy (paraphrased): students take action to protect their privacy on their devices and manage their personal data and security online, including their logins.
- **ISTE Standards for Students 1.3.b** — Evaluate information (paraphrased): students judge whether digital content is accurate and where it really comes from before they trust it.
- **CSTA PK-12 Computer Science Standards (2026) MS-SYS-SE-33** — Paraphrased: evaluate common cyber attacks such as phishing and social engineering, how they take advantage of people, and basic ways to prevent them, such as strong passwords, multifactor authentication and spotting suspicious activity.
- **CSTA K-12 Computer Science Standards (2017) 2-NI-05** — Paraphrased: explain how physical and digital security measures protect electronic information.

Aligns with commonly used digital citizenship frameworks (ISTE Standards for Students) and with both the 2026 CSTA PK-12 and the 2017 CSTA K-12 computer science standards; Georgia districts can map it to their state computer science and digital literacy expectations and to local acceptable-use policies.

## **Lesson sequence · 45 minutes**

### **5'** **Warm-up**

- 1 Show slide 1. Ask students to think of the last message they got offering something free in a game or on their phone. No names of games needed.
- 2 Ask: What did it want you to do? Collect answers: click a link, log in, send a code, send items first.
- 3 Tell students every scam needs them to take one action, and today they will learn to spot that action before they take it.

**Say:** *Scammers are not after you because you are careless. They send the same message to thousands of players and wait for one person to be in a hurry. Today you are going to be the person who is not in a hurry.*

### **10'** **Mini-lesson**

- 1 Slide 2: The four hooks. Free currency or items, 'verify your account or lose it', fake giveaways ('send 200, get 2,000 back'), and 'I sent my code to you by mistake, read it back to me.'
- 2 Slide 3: Red flags. A countdown or threat, a link that is not the real site, a request for a password or code, a request to move the conversation to another app, a deal that only works if you send something first.
- 3 Slide 4: The code rule. Your one-time code is like a key that only works for a minute. Anyone who asks for it, even a friend's account, is trying to get into your account.
- 4 Slide 5: Check another way. Do not use the link or number in the message. Open the game or app yourself, or contact your friend by a different route you already know.
- 5 Slide 6: Report, block, tell. Report the account in the game or app, block it, and tell a trusted adult. If you already clicked or shared, tell someone right away and change your password.

**Say:** *Real game companies do not give out free currency through random chat links, and nobody who is actually helping you ever needs your code. If a message asks for your login or your code, that is the answer: it is a scam.*

## 15' Activity

- 1 Hand out Worksheet 1. In groups of 3-4, students read each of the 12 mock messages and highlight every red flag in one color and any 'looks real' clue in a second color (about 6 minutes).
- 2 Groups sort each message into Scam, Probably fine or Check first and write a short 'why' for each (about 5 minutes).
- 3 Each group sends one person to the board to place two messages in the correct column, especially the Check first ones (about 2 minutes).
- 4 Quickly compare the board with the answer key and fix any misplaced items together (about 2 minutes).

**Say:** *Check first does not mean 'probably a scam.' It means the message might be real, but you will not use its link or trust it until you check another way.*

## 10' Discussion

- 1 Give each group two scenario cards. Groups decide what the student in the card should do and share one card with the class (about 5 minutes).
- 2 Use two discussion questions, starting with the hacked cousin's account and why a message from a friend can still be a scam (about 4 minutes).
- 3 Remind students that nobody gets in trouble for reporting, even if they already clicked. The faster an adult knows, the easier it is to fix (about 1 minute).

## 5' Exit ticket

- 1 Students answer the three exit ticket questions on a sticky note.
- 2 Hand out the crossword for early finishers or homework, and send home the family take-home sheet.

### Discussion questions

#### 1. Your cousin's account sends you 'omg is this you in this video' with a short link. Why can a message from someone you know still be a scam?

Listen for: Accounts get taken over, and scammers use them to message friends because people trust friends. The fix is to check with the cousin another way (text, call or in person) and not click the link.

#### 2. Why do scam messages almost always include a countdown, a threat or a 'first 50 only' limit?

Listen for: Pressure makes people act before they think. Students connect urgency to skipping the check-another-way step.

#### 3. Someone asks you to read back a code that was texted to you 'by mistake.' What is really happening?

Listen for: The person is trying to log in to your account, the site texted you the code, and they need it to finish getting in. Never share it; change your password because they may already have it.

#### 4. What makes the in-game news notice 'probably fine' while the free-gems chat message is a scam?

Listen for: The notice is in the game's own menu, asks for nothing and has no link. The chat message comes from a player account, has a countdown and asks you to log in on an outside site.

#### 5. If you already clicked a link and typed your password, what are your next steps?

Listen for: Tell a trusted adult right away; open the real app and change the password; turn on two-step sign-in if it is offered; check if any items or friends were changed; warn friends not to click links from your account.

### Exit ticket

Answer on a sticky note. No names needed.

1. Name two red flags in a 'free currency' message. → **Any two of: a link to a site that is not the game's real site, a countdown or 'first 50 only', a request to log in or share a password, a sender that is a player account pretending to be staff, a deal where you send something first.**
2. Someone asks for the code that was just texted to you. What do you do? → **Do not share it, stop replying, report and block, change your password in the real app and tell a trusted adult.**
3. What does 'check another way' mean? → **Do not use the link or number in the message. Open the app or website yourself, or contact the person by a route you already know, such as calling or asking in person.**



### Support

- Give a red-flag checklist strip to keep beside the worksheet: hurry, free, link, login, code, send first.
- Start with the four clearest messages (free gems, code read-back, giveaway, coach's practice update) before the harder Check first items.
- Allow groups to sort physical message strips into three envelopes before writing the why.



### Extend

- Students write their own realistic scam message with five hidden red flags, then trade with another group to find them all.
- Students compare a real account-security email from a service they use (opened from the app, not a link) with a fake one and list three differences, without sharing account details.
- Research challenge: explain why sites ask for a one-time code at all, and why a code sent by text is weaker than a code from an app or a security key.



### Multilingual learners

- Pre-teach the words verify, expire, giveaway, code and block with icons on the board.
- Offer sentence frames: 'This is a scam because \_\_\_\_.' 'I would check first by \_\_\_\_.'
- Let students discuss in their home language and report in English with a partner. Share the Spanish family sheet with Spanish-speaking families, and point out that the same scams arrive in many languages.



### Accessibility

- Every mock message is written out in full words, so it works with screen readers and in large print. Red flags are not shown only by color.
- Students can mark red flags by underlining, circling or numbering instead of highlighting.
- Offer a word bank version of the crossword, and allow oral answers for the exit ticket.



### Family extension

**Spot the scam: a family talk about game and text scams.** Today your student learned how scammers target young gamers and phone users with free currency offers, fake giveaways, 'verify your account' threats and requests for the code that is texted when someone logs in. The most important rule: never share a password or a one-time code with anyone, even a friend. Please take 10 minutes to talk about it together.

Send home the family sheet (English and Spanish) included in this lesson pack.



### Follow-up: free 2-minute lesson

[k12cyberforward.com/learn/game-chat-scams](https://k12cyberforward.com/learn/game-chat-scams)

Project it for a quick review or share the link with families.  
Related Cyber Academy course: academy-students-6-8.

### Sources and further reading.

- FTC — What's a verification code and why would someone ask me for it?: <https://consumer.ftc.gov/consumer-alerts/2024/03/whats-verification-code-why-would-someone-ask-me-it>
- FTC — How To Recognize and Avoid Phishing Scams: <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>
- CISA Secure Our World — Recognize and Report Phishing: <https://www.cisa.gov/secure-our-world/recognize-and-report-phishing>
- FTC — Avoiding and Reporting Gift Card Scams: <https://consumer.ftc.gov/articles/avoiding-and-reporting-gift-card-scams>
- CFPB — Consumer advisory: Video games are targeting your children to get into your wallet: <https://www.consumerfinance.gov/about-us/newsroom/consumer-advisory-video-games-are-targeting-your-children-to-get-into-your-wallet>
- NCMEC NetSmartz — Gaming: <https://www.missingkids.org/netsmartz/topics/gaming>
- ISTE Standards for Students: <https://iste.org/standards/iste-standards-for-students>
- CSTA — 2026 PK-12 Computer Science Standards: <https://csteachers.org/pk12standards/>