

CLASSROOM LESSON · GRADES 3-5

Tricks and traps online

Spot the red flags in free offers, fake prizes, fake friends and too-real pictures

Students learn the most common tricks they meet in games, videos and messages: free game currency offers, fake prize pop-ups, messages pretending to be a friend, requests for personal information and AI-made pictures that look real. They practice naming the red flag in each trick and choosing a safe move: pause, check with a trusted adult and use the real app or a known route.



GRADE BAND
3-5

TIME
45 minutes

FORMAT
Whole class + groups

PREP
Print & cut, ~10 min



BIG IDEA

Tricks want you to hurry, keep a secret or hand over something. When you spot a red flag, pause and check with a trusted adult before you click, share or believe.



Students will be able to

- ☐ Name at least five red flags (too good to be true, hurry, keep it secret, asks for a password or code, asks for personal information, wants to move to another app)
- ☐ Explain why a message from a friend's account might not really be from the friend, and how to check
- ☐ Explain that a picture or video can be made or changed by a computer, so a picture alone is not proof
- ☐ Choose a safe next step for a tricky situation, including telling a trusted adult if they already clicked or shared



Materials

- Board or projector for the slides
- Worksheet: Tricky moments (scenarios, 1 per student)
- Worksheet: Match the trick to the red flag (1 per student)
- Scenario cards (1 set per group of 4)
- Chart paper titled Red flags for the class list
- Sticky notes for the exit ticket
- Timer

Before class

- Print both worksheets and one set of scenario cards per group of four. Cut the cards apart.
- Write the Pause, Check, Choose steps on the board: Pause (hands off). Check (Is there a red flag? Can I check through the real app or a trusted adult?). Choose (close it, block or report, or keep going if a trusted adult confirms).
- Put chart paper titled Red flags on the wall; you will fill it in during the mini-lesson.
- Write the names of your trusted school adults on the board (teacher, counselor, library media specialist, school technology helper).
- Optional: decide which reporting steps your school uses for students (tell the teacher, use the report button in school apps).



Vocabulary

- **Scam** — A trick to get your money, your password, your account or your personal information.
- **Red flag** — A warning sign that something might be a trick, like a message that says hurry or keep this secret.
- **Personal information** — Facts about you that can help someone find you or pretend to be you: full name, address, school, birthday, phone number, passwords and photos.
- **Pretending (impersonation)** — When someone acts like they are a friend, a game company or the school when they are not.

Vocabulary (continued)

- **AI-made picture** — A picture, video or voice made or changed by a computer program. It can look or sound real even when it is not.
- **Login code** — A short number sent to a phone or email to prove it is really you. Never share it with anyone.

Standards alignment

- **ISTE Standards for Students 1.2.c** — Digital Citizen, Safeguard Well-being: students look after their well-being by making careful, purposeful choices about what they do online.
- **ISTE Standards for Students 1.2.d** — Digital Citizen, Digital Privacy: students take steps to protect their privacy on devices and look after their personal information and account security when they are online.
- **CSTA PK-12 Computer Science Standards (2026) E3-SYS-SE-13** — Grade 3, Systems and Security: students judge how sharing information online could give away personally identifiable information and other details about them.
- **CSTA PK-12 Computer Science Standards (2026) E3-SOC-ET-17** — Grade 3, Computing and Society: students describe how new technologies bring both helpful uses and risks to personal and family life.
- **CSTA K-12 Computer Science Standards (2017) 1B-NI-05** — Grades 3-5, Networks and the Internet: students talk about real cybersecurity problems and the ways people can protect personal information.

This lesson lines up with widely used digital citizenship and computer science frameworks; Georgia districts can map it to their state computer science and digital literacy expectations for grades 3-5.

Lesson sequence · 45 minutes

5' Warm-up

- 1 Read this out loud: "FREE 10,000 GEMS. Only 3 left. Log in now with your username and password to claim them."
- 2 Ask students to turn and talk: Would you click? What makes you want to? What makes you stop?
- 3 Collect two or three ideas. Write the first red flags on the chart paper (free stuff, hurry, asks for password).

Say: "Raise your hand if you have ever seen an ad or a pop-up that promised something free. Lots of hands. Today we are going to be trick detectives. Tricks online are made to look exciting, so it's not silly if you felt like clicking. The skill is noticing the red flag before your finger moves."

10' Mini-lesson

- 1 Slide 2, free game currency: Real games give items inside the game. Websites or videos that promise free gems, coins or skins if you type your login are trying to take your account. Red flags: too good to be true, asks for password.
- 2 Slide 3, fake prize pop-ups: "You are the 1,000,000th visitor" or "You won a phone." Real prizes do not ask you to tap fast, pay a fee or type personal information. Red flags: hurry, prize you did not enter for, asks for info.
- 3 Slide 4, fake friends: A message from a friend's account might be from someone who took over the account. Watch for "Is this you in this video?" with a link, or "I'm locked out, send me the code that just came to your phone." Check by asking the friend in person or a different way, with a trusted adult.
- 4 Slide 5, personal information: Fun quizzes like "Your superhero name is your street plus your birthday month" can collect personal facts. Keep full name, address, school, birthday, phone number, passwords and photos private.
- 5 Slide 6, AI-made pictures: Computer programs can now make pictures, videos and voices that look and sound real. Sometimes there are clues, like odd hands or blurry words, but many have no clues at all. So ask: Who posted it? Does it want me to click, buy, share or feel a big feeling? A picture is not proof.
- 6 Slide 7, the safe move: Pause, Check, Choose. Add each red flag to the chart as you go. Finish with: If you already clicked or shared, tell a trusted adult right away. You are not in trouble.

Say: "Every trick wants one of three things: your account, your information or your money. And most tricks use the same few moves. They make you hurry. They promise something amazing. They ask for a secret, like a password or a code. Or they ask you to keep it secret from grown-ups. When you see one of those moves, that's a red flag. Pause, check with a trusted adult, then choose."

18' Activity

- 1 Scenario card rotation (8 minutes): in groups of four, students take turns reading a card aloud. The group names the red flag and agrees on the safe move. One student records answers on scrap paper.
- 2 Tricky moments worksheet (6 minutes): students work alone or in pairs on the six scenarios, circling the best choice and writing the red flag.
- 3 Match the trick to the red flag (4 minutes): students draw lines to match each trick to its red flag. Early finishers write a new trick and its red flag on the back.
- 4 Circulate and listen for the key ideas: pause, check through the real app or a trusted adult, and tell even if you already clicked.

7' Discussion

- 1 Ask groups to share their hardest card and what they decided.
- 2 Use two or three discussion questions. Add any new red flags to the class chart.
- 3 Talk about how it feels to be tricked: it happens to adults too, and the smart move is telling fast so someone can help fix it.

5' Exit ticket

- 1 Students answer the three exit ticket questions on a sticky note.
- 2 Collect and sort into ready and needs a check-in; follow up with students who would share a code or believe a picture without checking.

Discussion questions

1. Why do tricks so often say hurry or only 3 left?

Listen for: Hurry makes people act before they think. Pausing takes away the trick's power.

2. Your friend's account sends you a link that says "LOL is this you?" How could you check if it is really your friend?

Listen for: Ask the friend in person, at school or with a trusted adult's help by phone. Don't click the link or reply with info first.

3. Why should you never share a login code, even with someone who says they are your friend?

Listen for: The code lets someone into your account. A real friend would never need it.

4. How can you decide whether to believe a picture or video that looks real?

Listen for: Check who posted it, whether a trusted source shares it, and whether it wants you to click, buy, share or feel scared. Ask a trusted adult. A picture alone is not proof.

5. What should you do if you already clicked a trick link or shared something?

Listen for: Tell a trusted adult right away so they can change passwords or report it. You are not in trouble.

Exit ticket

On your sticky note, answer all three.

1. Name two red flags. → **Any two: too good to be true, hurry, asks for a password or code, asks for personal information, keep it a secret, move to another app, a pay-first prize.**
2. A message from a friend's account says "I'm locked out. Send me the code that just came to your phone." What do you do? → **Don't send the code. Tell a trusted adult and check with the friend in person.**
3. Finish the sentence: If I already clicked, I _____. → **Tell a trusted adult right away.**



Support

- Give a red flag word bank (hurry, free, secret, password, code, personal info, new app, picture) for students to copy from.
- Reduce the scenarios worksheet to the first four items.
- Read scenario cards aloud for groups that need it, or assign a strong reader as card reader.
- Pre-highlight the red flag words in each card for students who need a visual cue.



Extend

- Students design a fake (harmless) trick poster with three red flags hidden in it for classmates to find.
- Students research one tip from the FTC page Kids and video games with a trusted adult and share it with the class.
- Students write a short guide for second graders called Stop, Think, Ask using words younger kids understand.
- Students write three questions they would ask before believing a surprising picture or video, then test their questions on Card 6 and share the best one with the class.



Multilingual learners

- Pre-teach key words with icons: free (gift), hurry (clock), secret (finger to lips), code (key), picture (camera).
- Spanish connections: estafa (scam), señal de alerta (red flag), información personal (personal information), código (code), adulto de confianza (trusted adult).
- Allow students to discuss the cards in their home language and report back in English, or the other way around.
- Provide sentence frames: "The red flag is ___ because ___." "The safe move is ___."



Accessibility

- Fine-motor needs: students can say their answers to a partner or adult scribe instead of writing; on the match worksheet they can say the letter or number instead of drawing lines.
- Visual needs: enlarge worksheets to 150 percent, read cards aloud, and describe each slide in words. The red flag list is written in words, not shown only with color.
- Offer a digital copy of the worksheets that works with a screen reader, if your school's learning management system allows it.
- Some students may have been tricked before and feel embarrassed. Keep the tone kind, avoid asking for personal stories in front of the class, and offer private check-ins.



Family extension

Tricks and traps online: a family page. Today your child learned to spot red flags in online tricks: free game currency offers, fake prizes, messages pretending to be a friend, requests for personal information and AI-made pictures that look real. The safe move is to pause, check with a trusted adult and use the real app. Children never get in trouble for telling.

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



Follow-up: free 2-minute lesson

k12cyberforward.com/learn/student-message-map

Project it for a quick review or share the link with families.

Related Cyber Academy course: academy-students-3-5.

Sources and further reading.

- FTC Consumer Advice: Kids and video games (keep personal details private; block players who ask personal questions; talk to a trusted adult): <https://consumer.ftc.gov/articles/kids-video-games>
- FTC Consumer Advice: Fake prize, sweepstakes and lottery scams (real prizes are free; act-now pressure): <https://consumer.ftc.gov/articles/fake-prize-sweepstakes-and-lottery-scams>
- CISA Secure Our World: Recognize and report phishing (urgency, too-good-to-be-true offers, impersonation, requests for personal information): <https://www.cisa.gov/secure-our-world/recognize-and-report-phishing>
- FTC Consumer Alert: Scammers use AI to enhance their family emergency schemes (voice cloning): <https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes>
- FTC Consumer Advice: Heads Up, Stop. Think. Connect.: <https://consumer.ftc.gov/articles/heads-up>
- ISTE Standards for Students: <https://iste.org/standards/for-students>
- CSTA 2026 PK-12 Computer Science Standards: <https://csteachers.org/pk12standards/>
- CSTA K-12 Computer Science Standards (2017), condensed: <https://csteachers.org/wp-content/uploads/2025/03/csta-k-12-computer-science-standards-revised.pdf>