

Module 7 of 9 · 0/3 lessons done · Quiz: not taken · 0%

[← Family course](#)

QUIZ NOT STARTED · pass mark 80%

Family Module 7 · Privacy & Safety · about 34 minutes · 3 lessons + 10-question quiz

Privacy and Safety

Trust, but verify. What to share, what never to share, how to spot scams, and how to check the assistant's work.

▶ Open slides

Download the PDF workbook

Exercises work with Grok Bot or any AI assistant. Use non-sensitive information only.
App connections marked "varies" depend on your school, team or provider and are confirmed during setup.

Lessons

Lesson 1 · What to share and what never to share (~9 min)

Lesson 2 · Spotting scams and fake messages (~9 min)

Lesson 3 · Checking the assistant's work (~8 min)

Module quiz (10 questions, ~8 min)

[Send feedback](#)

Lesson 1 · ~9 min

What to share and what never to share

You will be able to

- Sort information into OK, careful and never
- Keep passwords and codes out of chat

Your assistant works better with context, but some things never belong in a chat: passwords, one-time codes, full card or Social Security numbers. Sign-ins always happen on the official app or website.

Step by step

1. Make three columns: OK (schedules, grocery lists), Careful (health, kids' school details), Never (passwords, codes, card numbers, SSNs).
2. Tell the assistant: "Never ask me for passwords or codes in chat."
3. If you ever see a request for a code in chat or email, stop and check with a person you trust.
4. Review connected accounts every few months and remove ones you don't use.

Example

A message says "To finish connecting, reply with the 6-digit code we just texted you."
That's a red flag. Real connections use the provider's own sign-in screen.

Checklist

- ☐ I know my Never list
- ☐ My assistant knows never to ask for codes
- ☐ I've reviewed my connected accounts

Key points

- Passwords and codes never go in chat.

- Sign in on official pages only.
- Review connections a few times a year.

← Previous

Mark complete & next: Lesson 2 →

Lesson 2 • ~9 min

Spotting scams and fake messages

You will be able to

- Recognize common family-targeted scams
- Know how the assistant flags suspicious messages

Scammers love busy parents: fake package notices, fake school fees, 'urgent' gift-card requests from a 'principal'. The assistant can flag messages that look wrong, but you make the call.

Step by step

1. Ask the assistant to flag messages that ask for money, gift cards, codes or urgent action.
2. Check the sender's real address, not just the display name.
3. Call the school, bank or company using a number you already know, not one in the message.
4. Never let the assistant pay or reply to a flagged message.

Example

An email 'from the PTA' asks for \$50 in gift cards by noon. The assistant flags it: the address is a free webmail account and the PTA never asks for gift cards.

Checklist

- ☐ Scam flagging is turned on
- ☐ I check sender addresses
- ☐ I verify using known phone numbers

Key points

- Urgency plus money is a red flag.

- Verify through a channel you already trust.
- The assistant flags; you decide.

← Previous

Mark complete & next: Lesson 3 →

Lesson 3 • ~8 min

Checking the assistant's work

You will be able to

- Know when to double-check
- Build a quick verification habit

AI assistants are helpful and sometimes confidently wrong. A time can be misread, a portal flag can be stale. The higher the stakes, the more you check.

Step by step

1. For anything involving money, health or a deadline, open the original email or portal before acting.

2. Ask the assistant: "Where did you get that?" It should point to the source.
3. If something's wrong, tell it, so it can correct course.
4. Keep a short list of mistakes; patterns tell you what to fix.

Example

The digest says a project is missing. The portal shows it graded 100/100 yesterday. The flag was stale. Check before you nag.

Checklist

- ☐ I check the source on high-stakes items
- ☐ I ask 'where did you get that?'
- ☐ I report mistakes back

Key points

- High stakes, double check.
- Ask for the source.
- Correct it so it learns your setup.

Privacy and Safety quiz

10 questions, about 8 minutes. Pass mark 80%. Your best score is saved in this browser.

1. Which item belongs on the 'Never share in chat' list?

- ☐ Your grocery list
- ☐ Soccer schedule
- ☐ Dinner ideas
- ☐ One-time login codes

2. Where should sign-ins happen?

- ☐ On the official app or website's sign-in page

- ☐ In the assistant chat
- ☐ In an email reply
- ☐ In a text reply

3. A message asks you to reply with the 6-digit code you just got. What is it?

- ☐ A calendar invite
- ☐ A school requirement
- ☐ Normal setup
- ☐ A red flag for a scam

4. How often should you review connected accounts?

- ☐ Only if you're hacked
- ☐ Every few months
- ☐ Every hour
- ☐ Never

5. Which combination is a classic scam sign?

- ☐ A calendar update
- ☐ Urgency plus a request for money or gift cards
- ☐ A thank-you note
- ☐ A newsletter

6. How should you verify a suspicious request from the 'school'?

- ☐ Call using a number you already know
- ☐ Click the link
- ☐ Ask the assistant to pay it
- ☐ Reply to the email

7. What should the assistant do with a flagged message?

- ☐ Pay it
- ☐ Flag it for you and never pay or reply to it
- ☐ Forward it to everyone

☐ Delete your account

8. When should you open the original source before acting?

☐ Only for newsletters

☐ For anything involving money, health or a deadline

☐ Only on weekends

☐ Never

9. What should you ask when a summary looks off?

☐ 'Can you pay this?'

☐ 'Why are you so slow?'

☐ 'Where did you get that?'

☐ Nothing

10. Why report mistakes back to the assistant?

☐ So it can correct course and you can spot patterns

☐ To punish it

☐ It deletes the routine

☐ It's required by law

Check answers

[← Previous: Module 6](#)

[Next: Module 8 →](#)