

FREE COMMUNITY PROGRAM

**Spot the tactics.
Practice your response.**



PARTICIPANT COMPANION

A note from Dylan

A free, student-led community program built around calm, practical learning.

WHY I STARTED SCAMSAVVY

Hi, I'm Dylan Bagley, a junior at Arizona College Preparatory High School. I created ScamSavvy because I know people personally who have been affected by scams, and I've seen how big a problem scams have become. I wanted to make a difference in my community. ScamSavvy is a free community scam-awareness program, and I developed the website and tools that support the sessions.

AT A GLANCE

Dylan Bagley

Local high school junior

SCHOOL Arizona College Preparatory High School

BUILT BY DYLAN Website and tools for the workshop

The goal is simple: make space to notice pressure, pause, and practice a next step.

The 30-minute plan

Two live demos make room to see the steps, then practice them.

0-5 MIN

Why it matters

Start with everyday scam pressure.

5-12 MIN

Five tactics

Notice common ways a message pushes.

12-20 MIN

Check a Message

Watch the live message-check demo.

20-30 MIN

Practice Studio

Try a response in a guided scenario.

NOTES TO REVISIT

What do I want to remember or ask about later?

Five pressure patterns

These are ScamSavvy's teaching framework, not a complete checklist or proof that a message is fraudulent.

01

URGENCY



Pushes you to act before you can check.

EXAMPLE CUE

"Act now."

02

AUTHORITY



Pretends to be a trusted organization, official, or person.

EXAMPLE CUE

"I'm with your bank."

03

FEAR



Uses a threat or alarming claim to rush your choice.

EXAMPLE CUE

"Your account will close."

Two more patterns to notice

A useful clue tells you what to check next; it does not ask you to guess or accuse.

04

ISOLATION



Tries to keep you from checking with someone else.

EXAMPLE CUE

"Don't tell anyone."

05

REWARD



Offers a prize, refund, relationship, or unusually high return.

EXAMPLE CUE

"You've won."

ONE CLUE IS A PAUSE POINT

What can I verify using a contact method I choose?

Check a Message

Follow the message-check demo and note the clues before you see the tool's result.

PRACTICE MESSAGE / FICTIONAL

“We put your account on hold. Verify your details now or your order will be canceled.”

NO REAL LINK — PRACTICE ONLY

The sample is made for discussion. It is not a real company notice.

WATCH FOR THESE CHECKPOINTS

- 1 What does the sender want you to do?

- 2 Which pressure cues do you notice?

- 3 What could you check outside the message?

Use the tool's result as a prompt to check, not as a substitute for a source you trust.

Practice Studio

Work through a scenario together. The goal is to rehearse a calm next step.

PRACTICE SCENARIO / "THE PANICKED GRANDCHILD"

"Grandma, I need help right now. Can you send \$250 through Venmo? Please don't tell anyone until I get home."

PRESSURE TO NOTICE

Urgency • Money request • Secrecy

Name the pressure, then choose a way to verify independently.

WHAT WOULD YOU DO FIRST?

A CALM RESPONSE COULD BE

I'm going to call you on the number I already have saved before I send anything.

MY OWN WORDS

Notice. Pause. Verify.

A repeatable routine helps you make space before you respond.

1 NOTICE

What are they asking me to do? Which pressure patterns show up?

2 PAUSE

Do not click, pay, share, or stay on the line just because someone is rushing you.

3 VERIFY

Use a known number or site you find independently—not details from the message. [4]

MY PAUSE PLAN

If I feel rushed, I can first:

I can verify by:

If you already sent money

Act quickly and contact the provider. A reversal is not guaranteed, but it is worth asking. [4]

1 Stop the conversation

Do not send more money or share more information. Keep any receipts or messages you have.

2 Contact the payment provider now

Use the official app or the number on your card. Ask whether the payment can be stopped or reversed. [4]

3 Report it to the FTC

Use [ReportFraud.ftc.gov](https://reportfraud.ftc.gov). If you paid through a bank, card, payment app, wire, gift card, or crypto service, tell the provider how. [4]

4 If it involved the internet

You can also file a report at [IC3.gov](https://ic3.gov). IC3 says reports can support investigations and, in some cases, fund freezes. [1]

WATCH FOR RECOVERY IMPERSONATORS

IC3 says it never asks for money or partners with recovery firms. [6]

If you shared information or access

Use the real account provider's recovery path, not a link sent by the person who contacted you.

ACCOUNT LOGIN OR PASSWORD

- 1 Change the password**
Use the official site or app. Change it anywhere else you reused it. [4]
- 2 Add a second check**
Turn on two-factor authentication if the account offers it. [4]
- 3 Locked out?**
Use the provider's official account recovery steps. [4]

PERSONAL INFORMATION

If you think someone is using your identity, start at IdentityTheft.gov for a free recovery plan. If you shared a Social Security number, follow the site's steps to help protect your identity. [4, 5]

DEVICE ACCESS

If someone had access to your phone or computer, update security software, run a scan, and change passwords. Ask a trusted person or the device maker for help if needed. [4]

Help and source notes

Official starting points and sources checked for this booklet. Sources reviewed October 2026.

OFFICIAL HELP

REPORT A SCAM

ReportFraud.ftc.gov

REPORT INTERNET-ENABLED CRIME

IC3.gov

IDENTITY THEFT RECOVERY

IdentityTheft.gov

For immediate danger, call 911.

Use your bank, card issuer, or payment service's official contact details. [4]

SOURCE NOTES

[1] FBI Internet Crime Complaint Center (IC3), [2025 Annual Report](#), pp. 8–9. Annual data and cyber-enabled fraud reporting.

[2] FTC, [Protecting Older Consumers 2024–2025](#) (Dec. 1, 2025). Further reading on older-adult reports and FTC prevention work.

[3] Roozenbeek et al., [Psychological inoculation improves resilience against misinformation on social media](#), *Science Advances* 8(34), eabo6254 (2022), doi:10.1126/sciadv.abo6254. Related misinformation research; not a test of scams or ScamSavvy.

[4] FTC Consumer Advice, [What To Do if You Were Scammed](#) (June 2026).

[5] FTC Consumer Advice, [What To Know About Identity Theft](#) (Sept. 2024).

[6] FBI IC3, [Scammers are Impersonating the IC3](#). IC3 says it never works with recovery firms or directly asks for money.

