

Family pause checklist

Reviewed October 1, 2026

Use this one-page routine before anyone replies, clicks, calls back, shares a code, sends money, moves money, installs software, or scans a QR code from an unexpected request.

1. Set the pause rule

- No urgent money move without a second person.
- No one-time code, password, card number, account number, or identity number shared with an unexpected caller or message.
- No callback from a number inside an urgent message. Use a saved number, card, bill, official app, or website opened separately.

2. Pick two trusted contacts

- Contact 1:
- Contact 2:
- Backup contact:

3. Create a family safe word

- Pick a word or phrase that is easy for the family to remember and hard for outsiders to guess.
- Do not post clues about it online.
- Use it when a call or message claims someone needs urgent help.
- Still call a saved number to check the story; a familiar voice or safe word alone is not a guarantee.

4. Questions to ask out loud

- Who contacted me?
- What do they want me to do right now?
- Are they asking for money, a code, account access, or secrecy?
- Can I verify this through a path I already trusted before this message or call?
- What happens if I wait ten minutes?

5. If someone already acted

- Save screenshots, phone numbers, emails, receipts, account names, and dates.
- Contact the bank, card issuer, payment app, platform, or account provider directly.
- Report fraud attempts or losses at <https://reportfraud.ftc.gov/>
- Use identity recovery steps at <https://www.identitytheft.gov/> if identity information was shared.
- Use <https://www.ic3.gov/> for cyber-enabled losses, account takeover, online fraud, and related reports.

Olevo can be one optional second opinion for messages, screenshots, photos of notices, and typed call details. It does not replace direct verification with the real provider, agency, platform, or trusted contact.

Sources and sharing

FTC family-call guidance: <https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes>

FTC recovery guidance: <https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>

Prepared by Olevo / Infral Labs LLC for education; no agency endorsement. Print and share unchanged with credit, date, and sources. Label adaptations. Updates: <https://olevo.app/community-resources>

Library workshop checklist

Reviewed October 1, 2026

Goal: help participants practice one calm verification routine before responding to urgent messages, calls, screenshots, letters, or QR notices.

Before the session

- Print this checklist and the family pause checklist.
- Choose one example message, one call story, and one mailed-notice scenario.
- Keep examples fictional and avoid real names, full phone numbers, account numbers, and private documents.
- Put these source links on a handout or slide:
- FTC consumer alerts: <https://consumer.ftc.gov/consumer-alerts>
- **Report fraud:** <https://reportfraud.ftc.gov/>
- **Identity recovery:** <https://www.identitytheft.gov/>
- **FBI IC3:** <https://www.ic3.gov/>

15-minute format

- Read one example out loud.
- Ask: what is the sender asking for?
- Ask: what pressure is being used?
- Pick a trusted verification path that does not use the message link or callback number.

30-minute format

- Add a safe-word exercise for family emergency calls.
- Practice saying: "I need to verify this through a saved contact first."
- Practice ending a call without arguing.

45-minute format

- Add a reporting and recovery exercise.
- Match scenarios to the first reporting path:
- **Fraud attempt or money loss:** ReportFraud.ftc.gov
- **Identity information shared:** IdentityTheft.gov
- **Cyber-enabled loss or account takeover:** IC3.gov
- Bank, card, or payment app issue: contact the provider directly

Facilitation notes

- Do not blame the person who received the message. The pressure is the tactic.
- Keep the lesson practical: one pause rule, one saved contact path, one reporting link.
- Remind participants not to write passwords, one-time codes, full card numbers, account numbers, or identity numbers on public worksheets.

Olevo can be mentioned as one optional second opinion, but the workshop works without promoting any app.

Sources and sharing

FTC library education resources: <https://consumer.ftc.gov/features/librarians>

FTC recovery guidance: <https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>

Session lengths are suggested activities, not tested learning outcomes. Prepared by Olevo / Infral Labs LLC; no agency endorsement. Print and share unchanged with credit, date, and sources. Label adaptations. Updates: <https://olevo.app/community-resources>

Community reporting checklist

Reviewed October 1, 2026

Use this handout after a suspicious message, call, website, payment request, account alert, mailed notice, or QR code.

First, stop the urgent action

- Do not send more money.
- Do not share more codes, passwords, card numbers, account numbers, or identity numbers.
- Do not install remote-access software.
- Do not call back using the number in the urgent message.

Save useful evidence

- Screenshots of messages, emails, profiles, websites, QR notices, and payment requests.
- Phone numbers, email addresses, usernames, websites, wallet addresses, invoice details, tracking numbers, or order numbers.
- Dates, times, payment methods, receipt numbers, and the amount requested or sent.
- A short description of what the person or message asked you to do.

Choose the first reporting path

- Fraud attempts or money losses: <https://reportfraud.ftc.gov/>
- Identity information shared: <https://www.identitytheft.gov/>
- Cyber-enabled loss, account takeover, online fraud, or crypto transfer: <https://www.ic3.gov/>
- Mail fraud or suspicious mailed notices: <https://www.uspis.gov/report>
- Local immediate danger: call local emergency services.
- Bank, card, payment app, marketplace, email, or social account: contact that provider directly through its official app, website, or saved support number.

Recovery notes

- Payment recovery depends on the payment method and how quickly the provider is contacted.
- No outside person can promise to recover lost money for an upfront fee.
- Use a different trusted device when changing passwords if the affected device may be compromised.
- Turn on two-factor authentication where available, but never share one-time codes with unexpected contacts.

Group-use reminder

This handout is educational. It is not legal, financial, law-enforcement, medical, or emergency advice. For account, money, identity, or safety issues, contact the relevant provider, agency, or emergency contact directly.

Sources and sharing

FTC recovery guidance: <https://consumer.ftc.gov/articles/what-do-if-you-were-scammed>

FBI reporting guidance: <https://www.ic3.gov/>

Prepared by Olevo / Inftral Labs LLC; no agency endorsement. Print and share unchanged with credit, date, and sources. Label adaptations.

Updates: <https://olevo.app/community-resources>