

Personal Scam Protection Workbook

A free printable companion to *The Scam Survival Guide for Seniors* by Constantine Leith.

Print these pages, fill them in by hand, and keep them near your phone or with your financial papers. Once a year, go through them and update anything that has changed.

Don't write passwords, PINs, or verification codes anywhere in this workbook.

Your Three-Step Rule

Write this somewhere you'll see it:

STOP. CHECK. VERIFY.

When something feels urgent, **stop**: don't send money, don't share a code, don't click the link, and don't let anyone rush you. Then **check** what you're actually being asked to do. Finally, **verify** it through a source you trust.

Your Trusted Contacts

Choose two or three people you can call when something feels wrong. They don't need to be financial experts. They just need to be calm and easy to reach.

Trusted Contact 1

Name: _____

Relationship: _____

Phone: _____

Trusted Contact 2

Name: _____

Relationship: _____

Phone: _____

Trusted Contact 3

Name: _____

Relationship: _____

Phone: _____

Keep this page near your phone or somewhere else easy to find.

Your Financial Callback Numbers

Write down the official numbers for your main banks and cards. Take them from official websites, statements, the back of your cards, or your branch — never from a suspicious message.

Main Bank

Institution / service: _____

Official phone number: _____

Credit Card

Institution / service: _____

Official phone number: _____

Second Bank or Card

Institution / service: _____

Official phone number: _____

Payment App or Service

Institution / service: _____

Official phone number: _____

Your Family Emergency Plan

Agree on one simple rule: if someone calls or messages asking for emergency money, nobody sends anything until the request has been checked.

Family Safe Word

Safe word: _____

Pick something hard to guess. Avoid pet names, birthdays, street names, school names, and family names.

Your Family Verification Rule

1. End the call or message.
2. Call the person back on the number you already have.
3. If they don't answer, call another family member.
4. Use the family safe word if needed.
5. Don't send any money until the story is confirmed.

Your “Never” List

- ☐ I will not share a verification code.
- ☐ I will not give out my banking password.
- ☐ I will not share my PIN.
- ☐ I will not move money to a “safe account.”
- ☐ I will not buy gift cards for a stranger.
- ☐ I will not send cryptocurrency because someone called me.
- ☐ I will not give anyone remote access to my computer.
- ☐ I will not hand cash or gold to a courier.
- ☐ I will not hide a financial transaction from my bank or my family.
- ☐ I will not make a large payment while someone is pressuring me.

Your “Call Me First” Rule

Choose the amounts or situations that will automatically trigger a second opinion:

- ☐ Any transfer over \$_____
- ☐ Any gift card purchase for someone else
- ☐ Any cryptocurrency payment
- ☐ Any request from a new phone number
- ☐ Any investment introduced online
- ☐ Any request to keep a payment secret

Write your rule here:

Your Important Accounts

Email

Provider / institution: _____

Two-factor authentication or alerts on? Yes / No

Bank

Provider / institution: _____

Two-factor authentication or alerts on? Yes / No

Credit Card

Provider / institution: _____

Two-factor authentication or alerts on? Yes / No

Social Media

Provider / institution: _____

Two-factor authentication or alerts on? Yes / No

Payment Apps

Provider / institution: _____

Two-factor authentication or alerts on? Yes / No

Your Password Check

Do I use the same password for several important accounts? Yes / No

If yes, change the most important ones first: email, banking, payment apps, and social media.

Don't write your passwords in this workbook.

Your Email Security Check

- ☐ Strong password
- ☐ Different from my other passwords
- ☐ Two-factor authentication turned on
- ☐ Recovery phone number is correct
- ☐ Recovery email is correct
- ☐ No unknown forwarding rules
- ☐ No unfamiliar devices logged in

Your Bank Alert Check

Ask your bank which alerts it offers. Consider turning on alerts for:

- ☐ Large purchases
- ☐ Cash withdrawals
- ☐ Online transactions
- ☐ Transfers
- ☐ New payees
- ☐ Password changes
- ☐ Logins from a new device
- ☐ Changes to contact information

Your Device Check

- ☐ Automatic updates turned on
- ☐ Screen lock turned on
- ☐ Antivirus or security tools up to date
- ☐ Web browser up to date
- ☐ Any unknown remote-access software removed
- ☐ Important apps up to date

Your Social Media Check

- ☐ Who can see my phone number?
- ☐ Who can see my birthday?
- ☐ Who can see my family relationships?
- ☐ Who can see my home address?
- ☐ Who can see my travel plans?
- ☐ Who can contact me?
- ☐ Is two-factor authentication turned on?

You don't need to remove everything. Just cut back on what strangers could use to build a believable story.

Your Shopping Rule

- ☐ Check independent reviews
- ☐ Check the web address
- ☐ Compare the price with other sellers
- ☐ Avoid unusual payment methods
- ☐ Stay on the original platform when possible
- ☐ Never trust payment screenshots

Your Contractor Rule

- ☐ Get the estimate in writing
- ☐ Check out the company
- ☐ Verify the license if one is required
- ☐ Get a second estimate
- ☐ Avoid large upfront cash payments
- ☐ Never sign under pressure

Your Investment Rule

- ☐ Check out the company independently
- ☐ Find out who regulates it
- ☐ Understand how withdrawals work
- ☐ Never borrow to invest
- ☐ Never pay repeated fees to “unlock” money
- ☐ Never treat a dashboard as proof that the money exists
- ☐ Get a second opinion before any large transfer

Your Emergency Scam Card

Cut out this card and keep it by your phone.

IF SOMEONE ASKS FOR MONEY:

- Stop.
- Don't send anything.
- Don't share a code.
- Don't stay on the phone.
- Call back on a number you trust.
- Call someone you know.
- Verify first.

If You Think You Made a Mistake

1. Cut off contact.
2. Stop any further payments.
3. Call your bank or payment provider.
4. Change any exposed passwords.
5. Secure your email.
6. Disconnect any remote access.
7. Save the evidence.
8. Tell someone you trust.
9. Report the scam.
10. Watch out for recovery scams.

Your Scam Incident Notes

Date: _____

Time: _____

How did they contact you? Phone / Text / Email / Social Media / In Person

Name they used: _____

Company or agency they claimed to represent: _____

What did they ask you to do? _____

Did you send money? Yes / No Amount: _____

Did you share a password? Yes / No

Did you share a verification code? Yes / No

Did you install any software? Yes / No

Did you give anyone remote access? Yes / No

Who have you contacted so far? _____

Your Recovery Contacts

Bank Fraud Department

Name / institution: _____

Phone: _____

Credit Card Fraud Department

Name / institution: _____

Phone: _____

Trusted Family Contact

Name: _____

Phone: _____

Computer Technician

Name / company: _____

Phone: _____

Attorney or Financial Adviser

Name / firm: _____

Phone: _____

Annual Scam Safety Check

Once a year, go through this list:

- ☐ My trusted contacts are up to date.
- ☐ My bank and credit card phone numbers are up to date.
- ☐ My email has a strong, unique password.
- ☐ Two-factor authentication is on wherever it's offered.
- ☐ My bank alerts are active.
- ☐ My recovery phone numbers and emails are correct.
- ☐ Old or unknown logged-in devices have been removed.
- ☐ My social media privacy settings still make sense.
- ☐ Our family safe word is still private.
- ☐ Everyone knows our family "call me first" rule.
- ☐ No remote-access software is installed unless I use it on purpose.
- ☐ Scam-reporting resources are easy to find.

Personal Emergency Contact Sheet

Trusted person 1: _____

Phone: _____

Trusted person 2: _____

Phone: _____

Main bank: _____

Phone: _____

Credit card: _____

Phone: _____

Computer technician: _____

Phone: _____

Local police non-emergency: _____

Phone: _____

Family safe word stored securely? Yes / No

Other: _____

Phone: _____

Don't write passwords, PINs, or verification codes on this page.