SU BELLA VIDA · EDUCATIONAL SERIES

Financial Scams

Protecting a Lifetime of Hard-Earned Wealth

A practical guide and family defense workbook for older adults and their families

Comprehensive Edition · September 2026

SuBellaVida.Com

© 2025–2026 Su Bella Vida. All rights reserved.

Your Beautiful Life.

SuBellaVida.Com

Important Disclaimers

EDUCATIONAL TOOL NOTICE

This publication is provided by Su Bella Vida for educational and discussion purposes only. It is a learning resource to help readers recognize common financial scams, protect accounts and identity, and build a family response process. It is not a substitute for advice from licensed professionals, or for guidance from law-enforcement or consumer-protection agencies.

This book is not legal, tax, insurance, investment, cybersecurity, or law-enforcement advice. It is not a recommendation of any particular product, account, monitoring service, or institution. Scam tactics change constantly.

Su Bella Vida is not a bank, broker-dealer, registered investment advisor, CPA, enrolled agent, insurer, or law firm. We do not investigate fraud, recover funds, or practice law.

If you believe you have been scammed, contact your financial institution immediately and consider reporting to appropriate authorities. Do not send additional money to anyone claiming they can recover a prior loss.

Do not record passwords, PINs, recovery codes, or other secrets in this book or on printed worksheets. Keep credentials in a reputable password manager or other protected system.

Examples, checklists, and worksheets are educational illustrations, not guarantees. Always do your own research. You use this material at your own risk. Su Bella Vida is not responsible for decisions made on the basis of this publication.

Learn more at https://subellavida.com. Terms and disclaimer: https://subellavida.com/terms/. Support: support@subellavida.com.

By using this book you acknowledge that Su Bella Vida is a learning and organization tool, not a provider of professional financial, legal, or tax services. Read the current terms at subellavida.com/terms/ before relying on any planning discussion in these pages.

SuBellaVida

About This Book

A lifetime of disciplined saving can produce substantial retirement wealth—and that wealth can also become a target. Older adults may be targeted through government impersonation, fake investments, romance scams, family-emergency scams, Medicare fraud, contractor fraud, technology scams, and financial exploitation.

The risk is not a lack of intelligence. Sophisticated scams are designed around trust, authority, urgency, and isolation.

The second half of the book is a family operating system: two-person rules, continuity between spouses, secure records, quarterly reviews, and an annual fire drill.

The objective is protection without unnecessary loss of autonomy. Checks and balances are not distrust; they are continuity.

How to use this book

- Read the golden rule and impersonation chapters first.
- Use the family-system chapters as a household meeting agenda.
- Complete the companion worksheet together. Do not store passwords on the printed pages.
- Keep the family quick card visible. Revisit quarterly, and run an annual financial fire drill.

SuBellaVida.Com

Contents

Twenty chapters, then a companion worksheet, family quick card, and conclusion.

SuBella Vida.Com

1. Why Accumulated Wealth Attracts Scammers

• Retirement accounts, brokerage assets, home equity, pensions and long-established bank accounts can make a household an attractive target.

• Scammers may exploit fear, grief, loneliness, trust in authority, concern for children or grandchildren, or the desire to solve a problem quickly.

• The objective is often to make the victim believe that immediate action is required.

KEY TAKEAWAY

Financial sophistication does not eliminate scam risk. A strong system is more reliable than memory or vigilance alone.

SuBellaVida.Com

2. The Golden Rule: No Major Decision Under Pressure

- Never move retirement money, sell investments, wire money, buy cryptocurrency, buy gift cards, change beneficiaries, disclose credentials or give remote computer access because someone created an emergency.
- A legitimate institution can usually tolerate a pause for independent verification.
- Create a household rule: no major financial transaction happens without verification.

KEY TAKEAWAY

Urgency is a reason to slow down, not speed up.

SuBellaVida.Com

3. Government, IRS, Social Security and Medicare Impersonation

• Scammers may claim to represent the IRS, Social Security Administration, Medicare, police, courts, immigration authorities or other agencies.

• Threats may include arrest, benefit suspension, account seizure, lawsuits or legal action.

• Payment demands may involve gift cards, cryptocurrency, wire transfers or unusual payment channels.

KEY TAKEAWAY

End the conversation and independently contact the agency through an official channel.

SuBellaVida.Com

4. Bank, Brokerage and Financial-Institution Impersonation

- A scammer may know your name, bank and partial account information and claim suspicious activity has occurred.
- They may ask for a verification code, credentials or a transfer to a 'secure' account.
- A caller ID or a familiar-looking number is not proof of identity.

KEY TAKEAWAY

Call the institution using the number on your card, statement or official website. Never move money to protect it because an unsolicited caller told you to.

SuBellaVida.Com

5. Investment Fraud and Fake Financial Professionals

• Investment fraud can be especially destructive when retirement assets are involved.

• Examples include Ponzi schemes, fake advisers, unregistered investments, private-placement fraud, fake real estate deals, cryptocurrency platforms, guaranteed-return schemes and fake trading systems.

• Warning signs: guaranteed returns, little or no risk, secrecy, exclusivity, urgency, complex explanations, unclear custody, inability to withdraw money or personal payment instructions.

KEY TAKEAWAY

Verify the adviser, firm, investment and custodian independently before committing substantial funds.

SuBellaVida.Com

6. Romance and Relationship Financial Exploitation

- A scammer may build trust for months before requesting money.
- Stories may involve medical care, travel, legal problems, business opportunities or investments.
- The emotional relationship can make normal skepticism feel disloyal.

KEY TAKEAWAY

Do not send substantial funds to an online relationship you cannot independently verify. Discuss concerns with someone outside the relationship.

SuBellaVida.Com

7. Grandchild, Child and Family-Emergency Scams

- A caller may claim to be a grandchild or child who needs urgent help.
- Requests can involve bail, medical care, travel, gift cards, cryptocurrency or wire transfers.
- Voice cloning and compromised accounts can make impersonation more convincing.

KEY TAKEAWAY

Call the relative directly using a known number. Consider a private family verification phrase.

SuBellaVida.Com

8. Medicare, Health and Insurance Scams

- Scammers may request Medicare numbers, Social Security numbers, insurance information or banking details.
- They may promise free equipment, refunds, new benefits or special coverage.
- Unsolicited callers should not be trusted simply because they know basic personal details.

KEY TAKEAWAY

Verify the organization independently and do not provide sensitive information to unexpected callers.

SuBellaVida.Com

9. Home Repair, Contractor and Property Scams

• Door-to-door operators may claim a roof, driveway, tree, HVAC system or other property component needs immediate repair.

• Warning signs include immediate payment demands, cash-only terms, large deposits, no written contract, pressure to start immediately or refusal to provide references.

• Rental and property scams can also target owners and prospective renters.

KEY TAKEAWAY

Get multiple estimates, independently verify the contractor and use a written agreement.

SuBellaVida.Com

10. Technology, Phishing and Account-Takeover Scams

- Unexpected pop-ups and calls may claim a computer is infected or an account has been hacked.
- Scammers may request remote access, passwords, verification codes or payment.
- Email is particularly important because it can be used to reset other accounts.

KEY TAKEAWAY

Secure email and financial accounts with strong unique passwords, MFA, updated recovery information and transaction alerts. Never give an unsolicited caller remote access.

SuBellaVida.Com

11. Tax, Estate, Inheritance and Unclaimed-Asset Scams

• Scammers may claim you owe taxes, are receiving a refund, are under investigation, inherited money, won a prize or have unclaimed assets.

• They may demand legal fees, taxes, processing fees or bank information before releasing funds.

KEY TAKEAWAY

Do not send money to unlock an unexpected fortune. Verify claims through independent official or professional channels.

SuBellaVida.Com

12. Life Insurance, Annuity and Complex Financial-Product Scams

- A legitimate product is not automatically a good product, and a complicated product is not automatically fraudulent.
- Risk arises when a salesperson uses misrepresentation, pressure, hidden fees, unrealistic guarantees or complexity to prevent informed decision-making.
- Do not purchase a complex product during a single sales conversation.

KEY TAKEAWAY

Take documents home, compare alternatives, understand costs and consider independent advice.

SuBellaVida.Com

13. Cryptocurrency, Digital Assets and Recovery Scams

• Cryptocurrency transfers can be difficult or impossible to reverse.

• Warning signs include guaranteed returns, secret opportunities, romance plus investment, fake trading platforms, requests to move funds to a special wallet and people claiming they can recover prior losses.

• Recovery scammers often target people who have already lost money.

KEY TAKEAWAY

Never pay a recovery service simply because it promises certainty. Independently verify any recovery professional.

SuBellaVida.Com

14. Financial Exploitation by Someone You Know

• Financial abuse does not always come from strangers. Potential perpetrators can include caregivers, relatives, friends, romantic partners, contractors or people with access to accounts.

• Warning signs can include unexplained withdrawals, new financial relationships, sudden secrecy, beneficiary changes, unusual loans, large cash withdrawals or someone discouraging family contact.

KEY TAKEAWAY

These signs do not prove exploitation. They justify a respectful conversation and, when necessary, independent professional assistance.

SuBellaVida.Com

15. Build a Family Financial Defense System

- Designate trusted contacts where available.
- Use banking and investment alerts.
- Consider separating everyday spending money from long-term wealth.
- Use transfer limits and additional verification where available.
- Keep a secure inventory of institutions, assets and professional contacts.
- Make sure at least two trusted people understand the financial architecture.

KEY TAKEAWAY

The objective is protection without unnecessarily removing independence.

SuBellaVida.Com

16. Create a Two-Person Rule for Large Transactions

• Choose a household threshold appropriate to your circumstances.

• For example, any transfer above $10,000 could require a 24-hour pause and independent verification.

• The second person should know about the transaction—not necessarily have unrestricted access to the account.

• The rule should apply even when the request appears to come from a trusted person.

KEY TAKEAWAY

Checks and balances are especially valuable when emotions are high.

SuBellaVida.Com

17. Spouse-to-Spouse and Family Financial Continuity

• Both spouses should know where accounts are held, how bills are paid, what insurance exists, who the advisers are, where estate documents are stored and what major assets and debts exist.

• One spouse should not be the sole source of financial knowledge.

• The goal is not for everyone to manage everything. The goal is for the family to remain functional if the primary financial manager becomes unavailable.

KEY TAKEAWAY

Continuity planning is a core component of wealth protection.

SuBellaVida.Com

18. Emergency Financial Contact Sheet and Secure Records

• Maintain a secure inventory of banks, brokerage firms, retirement accounts, insurance, mortgage, CPA, attorney, financial adviser, estate documents, emergency contacts, major assets and digital assets.

• Do not place passwords in an unsecured spreadsheet or document.

• Use a secure credential system and establish an emergency-access procedure.

KEY TAKEAWAY

Keep enough information to locate and understand the financial system without creating a new security vulnerability.

SuBellaVida.Com

19. Quarterly Safety Review and Annual Financial Fire Drill

• Quarterly review: unfamiliar transactions, new accounts, unusual transfers, MFA, passwords, devices, credit activity, beneficiaries, estate documents, professional contacts and family continuity.

• Annual fire drill: ask whether the household could function if the person who manages finances were unavailable tomorrow.

• Test whether the second spouse or trusted person can identify income, accounts, bills, insurance, advisers, estate documents and important digital assets.

KEY TAKEAWAY

A system that has never been tested is only a plan on paper.

SuBellaVida.Com

20. What to Do If a Scam Happens

- Contact the bank, card issuer, brokerage, payment provider or other institution immediately.
- Ask about fraud procedures, recalls or reversals.
- Secure accounts and change compromised credentials.
- Review credit and consider appropriate fraud alerts or freezes.
- Document communications, transactions and evidence.
- Report the fraud through appropriate official channels.
- Tell family promptly. Do not let shame delay action.
- Be suspicious of anyone who offers guaranteed recovery for an upfront fee.

KEY TAKEAWAY

Speed, documentation and transparency can reduce the damage.

SuBellaVida.Com

Companion Worksheet & Checklist

SuBellaVida.Com

Family Scam-Defense Quick Card

- STOP — Do not act because someone created urgency.
- HANG UP — End unexpected calls requesting money or credentials.
- DON'T CLICK — Open official apps/websites yourself.
- VERIFY — Contact the institution or person independently.
- DISCUSS — For major transactions, involve the designated trusted person.
- REPORT — If fraud occurs, contact the financial institution immediately.
- NO SHAME — Tell the family early; speed can reduce damage.

SuBellaVida.Com

Conclusion

Financial security is not only about building wealth. It is about protecting the person, the accounts, the identity and the continuity of the financial plan. Scammers depend on speed, emotion and isolation. Families can counter those tactics with pause rules, independent verification, layered security, monitoring, trusted contacts and a culture in which asking 'Could this be a scam?' is considered responsible financial behavior.

SuBellaVida.Com

Companion Worksheet & Checklist

Use these pages as operating tools. Keep sensitive credentials outside these worksheets in a secure access system. Review at least annually and after a suspected incident.

WORKSHEET DISCLAIMER

These worksheets are educational templates, not legal forms. Completing them does not create a power of attorney, freeze credit, or constitute professional advice. Do not write passwords, PINs, or recovery codes here.

Family Scam-Defense Rules

Item	Done / notes
No major financial decision under pressure.	
Unexpected requests are independently verified.	
Major transactions are not secret from the spouse/family defense contact.	
Large transactions require a pause and second look.	
Passwords and MFA codes are never shared.	

Family Financial Map

Item	Done / notes
Primary bank: ____	
Savings / reserve: ____________________________________	
Brokerage: ____	
Retirement accounts: _________________________________	
Insurance: ____	
Mortgage / debt: ______________________________________	

Cpa: ____

Item	Done / notes
Attorney: ____	
Financial adviser: ____________________________________	

Large-Transaction Policy

Item	Done / notes
Threshold: $________________	
Waiting period: ______________	
Second person to be informed: ______________________________	
Exceptions, if any: ____	

Trusted Contacts & Continuity

Item	Done / notes
Primary trusted contact: ______________________________	
Backup trusted contact: ______________________________	
Spouse/partner who understands the plan: ______________	
Where the account inventory is stored: __________________	
Where estate documents are stored: ____________________	
Where digital-asset inventory is stored: ________________	

Quarterly Review

Item	Done / notes
Reviewed bank statements	
Reviewed investment statements	
Checked unusual transfers	
Checked credit activity	
Confirmed MFA/security	
Reviewed beneficiaries	
Confirmed professional contacts	
Confirmed spouse/trusted-person continuity	

Annual Financial Fire Drill

Item	Done / notes
Date: ___________________	
Could another trusted person locate the accounts? Yes No	
Could they identify how bills are paid? Yes No	
Could they contact the key professionals? Yes No	
Could they locate estate documents? Yes No	
Could they identify important digital assets? Yes No	
Actions required: ____	

SuBellaVida.Com

A closing note from Su Bella Vida

A lifetime of savings should not be undone by a hurried phone call. Families that pause, verify, and talk without shame give themselves time to protect the plan.

Su Bella Vida is designed to help you learn and organize—not to replace a CPA, attorney, fiduciary, bank fraud team, or law enforcement. When the plan is real, bring in the professionals who can put it into force.

Questions: support@subellavida.com · https://subellavida.com

SuBellaVida.Com