SU BELLA VIDA · EDUCATIONAL SERIES

Financial Scams

Protect Your Money, Identity, Credit and Future

A practical guide and family defense workbook for young adults

Comprehensive Edition · September 2026

SuBellaVida.Com

Your Beautiful Life.

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.

About This Book

Financial scams are not an issue reserved for retirees. Young adults are among the most digitally connected consumers, job seekers, students, renters, online shoppers, and new investors. That makes them attractive targets.

The damage can extend far beyond the initial dollar loss: stolen identity information can affect credit, housing, employment, insurance, and long-term financial continuity.

Each chapter names a pressure tactic, then translates it into a pause-and-verify habit. The companion worksheet and family quick card turn the reading into a working defense system.

Tactics change. The defense does not: never make an important financial decision under pressure, and independently verify unexpected requests.

How to use this book

- Start with the scam playbook if you are new to this topic.
- Skip to the scam type you just encountered if you need a fast check.
- Complete the companion worksheet and keep bank and credit-card contacts where you can find them without opening a suspicious message.
- Keep the family quick card visible. Tell a trusted person your plan so shame does not delay a report.

Contents

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

1. The Scam Playbook: How Criminals Get You to Act

• Urgency: 'Act now or your account will be closed.'

• Fear: threats of arrest, account loss, fraud or legal trouble.

• Authority: pretending to be a bank, government agency, employer, school, police officer or technology company.

• Greed: unusually high returns, prizes, giveaways or easy money.

• Emotion: romance, family emergencies, sympathy or guilt.

• Secrecy: instructions not to tell parents, friends, banks or employers.

• Isolation: moving you to a private chat, phone call or unfamiliar payment method.

• Trust exploitation: using information from social media, breached databases or previous conversations to sound legitimate.

KEY TAKEAWAY

The more a request combines urgency, secrecy and money, the more important it is to stop rather than comply.

2. Identity Theft and Personal-Information Scams

• Sensitive information includes Social Security number, date of birth, driver's-license or passport information, bank details, tax records, passwords, security questions, phone number and email credentials.

• Criminals may use identity information to open credit accounts, apply for loans, file fraudulent tax returns, obtain services, create accounts or impersonate you.

• Do not provide sensitive information merely because a caller or email looks professional.

• Ask why the information is needed, whether it can be provided through an official portal, and whether you initiated the interaction.

KEY TAKEAWAY

Use unique passwords, a password manager, multifactor authentication, device updates, credit monitoring/review and transaction alerts. Consider a credit freeze when appropriate.

3. Phishing, Smishing and Fake Messages

- Email phishing, SMS/text smishing and fake login pages are designed to capture credentials or payment information.
- Messages may imitate banks, retailers, delivery services, schools, employers, technology companies or government agencies.
- Links can lead to convincing copies of legitimate websites.
- Do not use the link in an unexpected message. Open the official app or type the known website address yourself.
- Never disclose a one-time verification code to someone who called or messaged you unexpectedly.

KEY TAKEAWAY

Treat unexpected messages as notifications to investigate, not instructions to obey.

4. Job, Gig and Work-From-Home Scams

• Fake jobs may promise unusually high pay for little work, skip normal interviews, use messaging apps exclusively, or ask applicants to pay for equipment or training.

• Fake employers may send a check and ask you to buy equipment, return money or forward funds.

• Criminals may recruit victims as money mules by asking them to receive and move money through personal accounts.

• A legitimate employer should not require your personal bank account to function as its payment-processing system.

KEY TAKEAWAY

Before accepting a job, independently verify the employer, domain, recruiter and role. Never forward money because a recruiter tells you to.

5. Fake Checks, Overpayments and Payment Reversals

- A scammer may send a check or electronic payment for more than the amount owed and ask you to return the difference.
- Money appearing in an account does not necessarily mean the underlying payment is final or legitimate.
- Victims can be left responsible when a fraudulent deposit is reversed.
- Do not refund an overpayment until your financial institution independently confirms the payment is legitimate and final.

KEY TAKEAWAY

Screenshots, emails and payment confirmations are not proof that funds are safely yours.

6. Romance, Friendship and Social-Engineering Scams

• Scammers may build relationships over weeks or months before introducing money.

• They may claim a medical emergency, travel problem, family crisis, legal issue or investment opportunity.

• They may discourage video calls, meetings or independent verification.

• The emotional bond is used to bypass normal financial judgment.

KEY TAKEAWAY

Never send money or cryptocurrency to an online relationship based only on trust built through messages. Talk to someone you trust before sending substantial funds.

7. Investment, Trading, Crypto and 'Easy Money' Scams

• Warning signs include guaranteed returns, no-risk claims, secret strategies, insider information, celebrity endorsements, AI trading claims, fake investment dashboards, pressure to deposit quickly and difficulty withdrawing funds.

• Fake platforms can display invented account balances and profits to encourage additional deposits.

• Recovery scammers may contact victims after an investment loss and promise to retrieve the money for an upfront fee.

KEY TAKEAWAY

Verify the person, firm, investment and custody of assets independently. Never invest because a stranger, social-media contact or unsolicited message created urgency.

8. Social Media, Influencer and Impersonation Scams

- A polished profile, blue check, follower count or mutual connections does not establish legitimacy.
- Scammers may impersonate friends, influencers, businesses, employers or public figures.
- Do not publish unnecessary personal information that can help answer security questions or impersonate you.
- If an account asks for money unexpectedly, verify through another established channel.

KEY TAKEAWAY

Assume an online identity is unverified until independently confirmed.

9. Online Marketplace, Shopping and Rental Scams

• Watch for fake payment confirmations, overpayment, requests to ship before payment clears, fake escrow services, counterfeit goods, unusually low prices and requests to move payment outside the platform.

• Rental scams may use copied listings and demand deposits before a legitimate showing or lease process.

• Use platform protections when available and independently verify ownership, business identity and payment instructions.

KEY TAKEAWAY

Never let a bargain or fear of losing a deal eliminate normal verification.

10. Government, Tax, Student-Loan and Benefits Scams

- Scammers impersonate the IRS, Social Security Administration, police, courts, immigration agencies, DMV, schools and student-loan services.
- They may threaten arrest, suspension, deportation, lawsuits or loss of benefits.
- Others promise student-loan forgiveness, scholarships or government programs in exchange for fees or sensitive information.

KEY TAKEAWAY

Do not use contact information supplied by the caller. Find the agency or program independently and contact it yourself.

11. Tech-Support, Account-Takeover and SIM-Swap Scams

• Unexpected pop-ups may claim your computer is infected and provide a phone number. Do not call it.

• Remote-access software can give a scammer control over your device and potentially expose credentials.

• Account takeover often begins with email because email can reset other accounts.

• SIM swapping attempts to move your phone number to a criminal's device so they can receive SMS codes.

KEY TAKEAWAY

Secure primary email first. Use strong unique passwords, MFA, recovery controls, carrier account PINs and stronger authentication methods where available.

12. Gift Cards, Wire Transfers, Cryptocurrency and Irreversible Payments

- Gift cards are a major warning sign when someone instructs you to buy them and provide the codes.
- Wire transfers and cryptocurrency can be difficult or impossible to reverse.
- Never allow someone to dictate the payment method simply because it is 'faster' or 'safer.'

KEY TAKEAWAY

Stop, verify the recipient independently, and use a protected payment mechanism when one exists.

13. Fake Charities and Emotional Causes

- Scammers exploit disasters, medical emergencies, wars, children in need and community tragedies.
- Use the charity's official website or another independent source to verify the organization.
- Do not donate because a message creates immediate emotional pressure.

KEY TAKEAWAY

Generosity should be intentional, not manipulated.

14. Family Emergency and 'Mom/Dad/Grandparent' Impersonation

• A scammer may claim to be a relative with a lost phone or urgent emergency.

• The scammer may request bail money, medical expenses, gift cards, cash, cryptocurrency or a wire transfer.

• Voice cloning and compromised messaging accounts can make impersonation more convincing.

> **KEY TAKEAWAY**
>
> Call the relative using a known number. A family verification phrase can add another layer.

15. Build Your Personal Scam Defense System

- Secure your primary email.
- Use a password manager and unique passwords.
- Enable multifactor authentication.
- Turn on bank and credit-card alerts.
- Review statements and credit activity.
- Consider a credit freeze when appropriate.
- Limit personal information on social media.
- Keep operating systems and apps updated.
- Never share passwords or one-time codes.
- Never let another person use your bank account to move money.

KEY TAKEAWAY

Your goal is layered defense: prevent, detect, respond.

16. The Five-Question Scam Test

- Who contacted me?
- How do I know they are who they claim to be?
- Why do they need me to act now?
- Can I verify the request independently?
- What happens if I wait 24 hours?

KEY TAKEAWAY

If you cannot independently verify the request, do not proceed.

17. What to Do If You Are Scammed

- Stop communicating with the scammer.
- Contact the bank, card issuer, payment service or investment firm immediately.
- Change compromised passwords and secure email.
- Ask financial institutions what fraud or reversal procedures are available.
- Review credit and consider a fraud alert or freeze where appropriate.
- Document dates, amounts, names, phone numbers, messages and transaction details.
- Report the fraud through appropriate official channels.
- Tell a trusted person. Do not hide the incident because of embarrassment.

KEY TAKEAWAY

Do not pay someone who promises to recover your lost money unless you have independently verified that service.

Companion Worksheet & Checklist

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.

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.

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.

My Scam-Defense Commitments

Item	Done / notes
I will pause when a request creates urgency.	
I will independently verify unexpected financial requests.	
I will never share passwords or MFA codes.	
I will not move money through my personal account for someone else.	
I will ask a trusted person before a major unfamiliar transaction.	

My Account Security Checklist

Item	Done / notes
Primary email has MFA.	
Password manager is in use.	
Banking alerts are enabled.	
Credit activity is reviewed.	
Important devices are updated.	
Recovery information is current.	

My Verification Contacts

Item	Done / notes
Bank: ____	
Credit-card issuer: __________________________________	
Primary financial institution: __________________________	
Trusted person: ______________________________________	
Mobile carrier: _______________________________________	

My Personal Red Flags

Item	Done / notes
Requests that should always make me pause: ________________________________	
Payment methods I will never use because of an unsolicited request: ____________	
People I will call before a major financial decision: _____________________________	

My Incident Plan

Item	Done / notes
If I suspect fraud, first call: __________________________	
Second person to notify: ______________________________	
Where I will keep evidence/screenshots: _________________	
Where I will keep official contact information: ____________	

A closing note from Su Bella Vida

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. A pause rule, independent verification, and one trusted person give you time.

Su Bella Vida is designed to help you learn and organize—not to replace a bank's fraud team, an attorney, or law enforcement. When money or identity is at risk, act quickly with the professionals who can put protections in force.

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