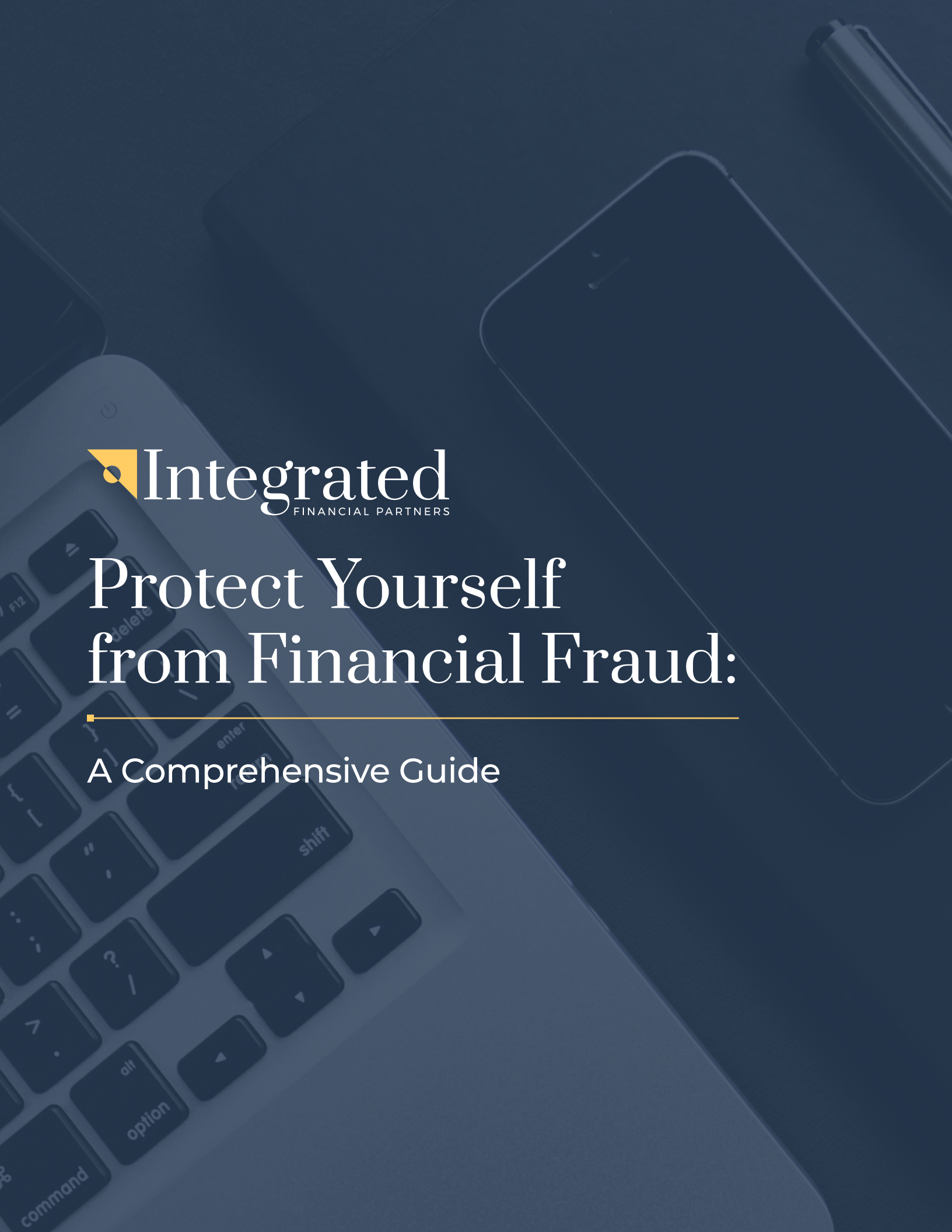

Integrated
FINANCIAL PARTNERS

Protect Yourself from Financial Fraud:

A Comprehensive Guide

INTRODUCTION

In today's digital age, cybercriminals are becoming increasingly sophisticated in their methods to exploit vulnerabilities and steal assets. While technology advances, so do the techniques used by fraudsters.

According to the Federal Trade Commission, people reported losing $10 billion to scams in 2023. That's $1 billion more than in 2022 and the highest ever in losses reported to the FTC, even though the number of fraud reports (2.6 million) was about the same as last year.[1]

This guide will help you protect yourself, your family, and your financial future through awareness and practical defensive strategies.

TRADITIONAL CYBER THREATS

Phishing: The Bait and Switch

Phishing remains one of the most prevalent cyber threats. Criminals impersonate legitimate institutions through emails, texts (smishing), or voice calls (vishing) to steal sensitive information or access accounts.

Enhanced Defense Strategies:

- Verify sender email addresses carefully, watching for slight misspellings or unusual domains.
- Never provide sensitive information in response to unsolicited communications.
- Use direct contact methods to verify suspicious requests.
- Enable spam filters and keep email security settings updated.
- Remember that legitimate institutions never request sensitive information via email.

Malware: The Silent Infiltrator

Modern malware has evolved beyond simple viruses to include sophisticated tools that can monitor activity, steal credentials, and even encrypt your files for ransom.

Protection Measures:

- Install and regularly update reputable antivirus and anti-malware software.
- Enable automatic updates for all operating systems and applications.
- Back up important files regularly to secure offline storage.
- Use ad-blockers and script-blockers in web browsers.
- Avoid downloading software from unofficial sources.
- Regularly scan external devices before connecting them to your network.

EMERGING THREATS

"Pig Butchering" Scams

This sophisticated form of fraud combines romance scams with cryptocurrency investment schemes. Scammers build trust over time before convincing victims to invest in fake platforms.

Warning Signs:

- Unsolicited messages on social media or dating apps from seemingly successful individuals.
- Conversations that quickly turn to investment opportunities.
- Pressure to move communications to private messaging apps.
- Claims of guaranteed returns or “insider” investment opportunities.
- Professional-looking but fraudulent investment platforms.

PHONE NUMBER SPOOFING AND REPLICATION

Criminals can now convincingly replicate phone numbers, making calls that appear to come from legitimate sources, including financial institutions or government agencies.

Protective Measures:

- Never trust caller ID alone to verify a caller’s identity.
- Establish a verbal password with your financial institution.
- End suspicious calls and dial known, verified numbers directly.
- Use call-blocking apps that filter known scam numbers.
- Register your number on the National Do Not Call Registry.

AI AND BIOMETRIC FRAUD

Artificial Intelligence has enabled sophisticated forms of deception, including deepfake videos and voice cloning technology that can create remarkably realistic impersonations. These tools pose risks not only for financial transactions but also for personal relationships, as scammers can now convincingly impersonate family members and friends.

Essential Safeguards:

- Establish personal verification codes with family members and friends to confirm identity during unexpected calls or video chats. These should be unique phrases or words that would be difficult for scammers to guess or find through social media.
- Implement mandatory video call verification for major financial transactions, ensuring the calls include specific security protocols and predetermined authentication steps.
- Create a multi-layered approach to biometric authentication, combining it with traditional security measures like passwords and physical tokens rather than relying on biometrics alone.
- Be skeptical regarding video or voice calls, particularly those involving urgent requests or demands for immediate action. Always verify through alternate communication channels.
- Set up enhanced voice authentication protocols with financial institutions, including specific security phrases or questions that go beyond standard verification methods.
- Develop a verification system for unusual requests that requires confirmation through multiple independent channels, whether dealing with financial institutions or personal contacts.
- Communicate with family and friends about your established security protocols so everyone understands and follows the agreed-upon verification methods.

FAMILY PROTECTION STRATEGY

Creating a Family Security Plan

Protecting your family requires coordination and shared awareness.

Key Components:

- Establish regular family discussions about current scams and security practices.
- Create an emergency contact list for financial institutions and law enforcement.
- Develop a process for verifying family members' urgent financial requests.
- Set up monitoring and alerts for elderly family members' accounts.
- Share approved contact methods and verification procedures with family members.

Digital Security Education:

- Teach children about online privacy and security from an early age.
- Help elderly family members recognize common scams.
- Create family protocols for sharing sensitive information.
- Regularly review and update security measures together.

RESPONSE PLAN: IF YOU BECOME A VICTIM

Immediate Actions

1. Contact your financial institutions immediately.
2. Place a fraud alert with credit bureaus (Equifax, Experian, TransUnion).
3. Change all passwords and security questions.
4. Contact your bank to initiate a credit fraud claim. (Most financial institutions have dedicated fraud protection insurance separate from FDIC coverage that can help recover funds lost through scams, unauthorized transfers, or compromised credit cards.)
5. Document everything: screenshots, emails, phone numbers, and conversations.

Official Reporting

1. File a police report.
2. Report to the FBI's Internet Crime Complaint Center (IC3).
3. Submit a complaint to the Federal Trade Commission (FTC).
4. Contact the IRS Identity Protection Unit if tax related.

Recovery Steps

1. Request new credit/debit cards and account numbers.
2. Monitor credit reports regularly.
3. Consider credit monitoring services.
4. Keep detailed records of all communications and recovery efforts.
5. Seek professional legal advice if significant losses occur.

PREVENTIVE SECURITY MEASURES

Strong Authentication

- Use password managers to generate and store complex passwords.
- Enable multi-factor authentication on all accounts.
- Consider hardware security keys for critical accounts.
- Update passwords regularly, especially after security incidents.

Network Security

- Use a VPN for public Wi-Fi connections.
- Regularly update home router firmware and settings.
- Separate networks for IoT devices and sensitive computing.
- Enable firewall protection on all devices.

STAYING INFORMED

Resources for Ongoing Education

- Subscribe to FTC scam alerts.
- Follow cybersecurity news sources.
- Join local community fraud awareness programs.
- Participate in security webinars offered by financial institutions.

Regular Security Check-ups to Conduct

- Monthly reviews of all financial statements.
- Quarterly credit report reviews.
- Annual security audits of digital accounts.
- Regular updates to family security plans.

CONCLUSION

Cybersecurity is an ongoing process, not a one-time solution. Stay vigilant, keep learning, and maintain open communication with our team and your family members. Remember that prevention is always easier than recovery, and when in doubt, verify before taking action.

If you have any questions about this material, please do not hesitate to reach out.

John H. Harrington, CFP®
Financial Planner
Integrated Financial Partners
44 Old Ridgebury Road, P-140, Danbury, CT 06810
TEL (845) 278-2629, Ext. 205 | FAX (845) 278-5463
John.Harrington@IFPadvisor.com | www.johnhharrington.com

[1] https://www.ftc.gov/business-guidance/blog/2024/02/facts-about-fraud-ftc-what-it-means-your-business