CSNP
CYBERSECURITY NON-PROFIT

Senior Cyber Threats Report 2025

A comprehensive analysis of cyber threats targeting older adults, examining emerging attack vectors, social engineering tactics, and evidence-based protective measures for the senior population.

CYBER SECURITY NON-PROFIT

2025 EDITION

EXECUTIVE OVERVIEW

The Growing Threat Landscape

Seniors represent a uniquely vulnerable demographic in today's digital threat environment. With $3.4 billion lost to fraud in 2023 alone, older adults face sophisticated attacks that exploit both technological unfamiliarity and social isolation.

This report examines the evolving tactics cybercriminals use to target seniors, from romance scams to tech support fraud, and provides actionable intelligence for security professionals protecting this population.

88K

Reported victims

Age 60+ in 2023

$3.4B

Total losses

Highest among age groups

THREAT CATEGORIES

Primary Attack Vectors Targeting Seniors

Romance & Confidence Scams

Criminals build emotional relationships over months, eventually requesting money for fake emergencies or investments.

Tech Support Fraud

Impersonating legitimate companies to gain remote access to devices and steal financial information.

Government Impersonation

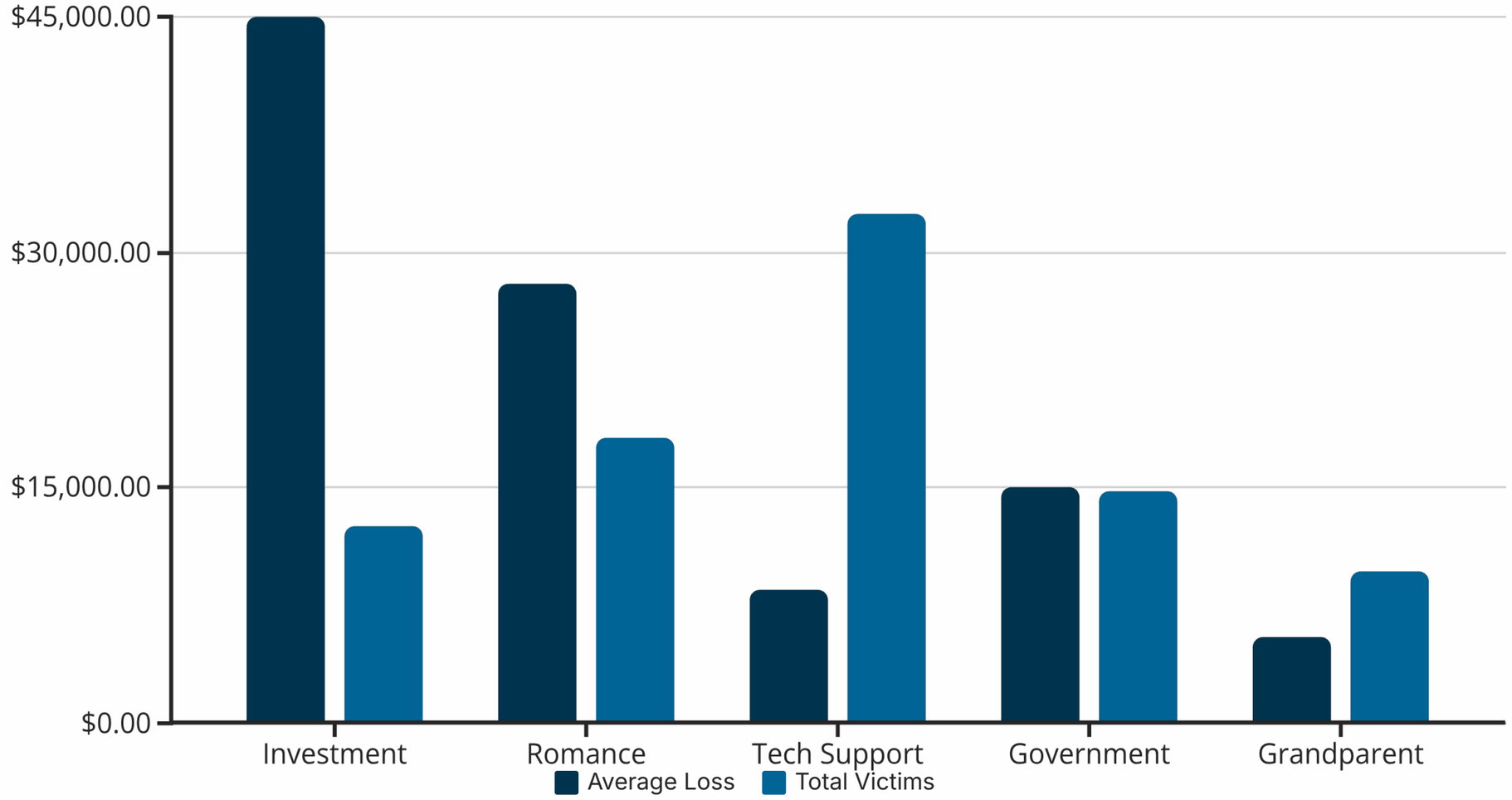
Posing as IRS, Social Security, or Medicare officials to intimidate victims into immediate payments.

Investment Schemes

Fraudulent cryptocurrency, real estate, or retirement investment opportunities promising unrealistic returns.

Financial Impact by Fraud Type

Analysis of reported losses reveals investment scams cause the highest individual losses, while tech support fraud affects the largest number of victims.



SOCIAL ENGINEERING TACTICS

Psychological Manipulation Techniques

Urgency Creation

Artificial deadlines and emergency scenarios pressure victims into acting without verification.

Authority Exploitation

Impersonating trusted institutions to bypass skepticism and establish immediate credibility.

Relationship Building

Investing weeks or months developing trust before introducing fraudulent requests.

Isolation Tactics

Discouraging victims from consulting family or advisors who might identify the scam.

Case Study: Multi-Stage Tech Support Attack

1 Initial Contact

Pop-up warning of virus infection with urgent phone number. Victim calls "support line" displayed on screen.

2 Remote Access

Scammer gains control via legitimate remote desktop software, displays fake scan results showing critical threats.

3 Payment Extraction

Victim charged $399 for unnecessary "protection service" using credit card over phone.

4 Secondary Attack

Follow-up call offering "refund" leads to fake bank login page, compromising banking credentials and additional losses.

VULNERABILITY FACTORS

Why Seniors Are Disproportionately Targeted

Digital Literacy Gap

Many seniors adopted technology later in life and may struggle to identify sophisticated phishing attempts, fake websites, or malicious software indicators that younger users recognize instinctively.

Financial Assets

Older adults often have accumulated savings, home equity, and retirement accounts, making them lucrative targets for criminals seeking substantial payouts from successful attacks.

Social Isolation

Loneliness makes seniors more susceptible to romance scams and more likely to engage with unsolicited callers or messages, seeking human connection.

Cognitive Decline

Age-related cognitive changes can impair judgment and decision-making, making it harder to detect inconsistencies in scammer stories or resist high-pressure tactics.

Trust Disposition

Generational differences in trust levels—seniors grew up in an era of greater institutional reliability—can be exploited by criminals impersonating authority figures.

Underreporting

Embarrassment and fear of losing independence prevent many seniors from reporting fraud, allowing criminals to continue operations and repeat attacks.

Emerging Threats: AI-Enhanced Attacks

Voice Cloning Scams

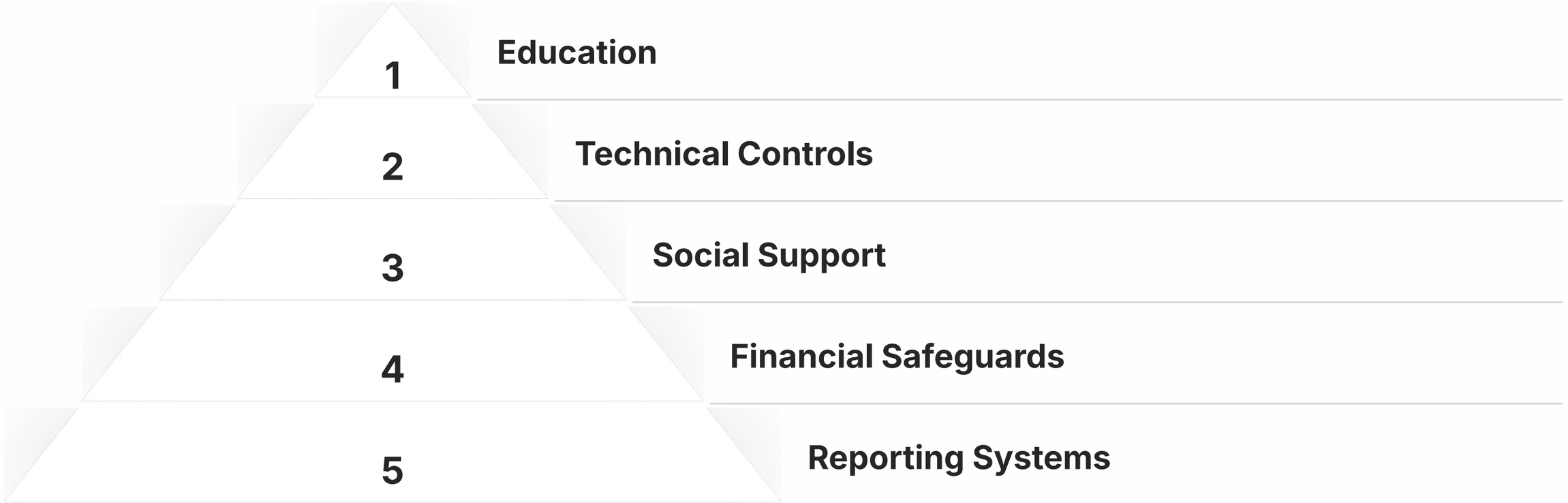
Artificial intelligence now enables criminals to clone voices from short audio samples found on social media. Scammers call seniors pretending to be grandchildren in distress, using synthesized voices that sound identical to their loved ones.

In 2024, voice cloning scams increased 400% year-over-year, with average losses exceeding $11,000 per incident. The emotional manipulation combined with authentic-sounding voices makes these attacks particularly devastating.

Red Flag: Any urgent request for money—especially via wire transfer, gift cards, or cryptocurrency—should be verified through a separate, known contact method, even if the voice sounds authentic.

DEFENSE STRATEGIES

Multi-Layered Protection Framework



Effective senior protection requires coordinated efforts across awareness training, device security, family communication, banking controls, and streamlined fraud reporting mechanisms. No single measure suffices—layered defenses create resilience.

Recommended Security Controls for Organizations

01

Implement Targeted Education Programs

Develop age-appropriate training covering common scams, red flags, and verification procedures using non-technical language and repetition.

02

Deploy Technical Safeguards

Install call-blocking technology, email filtering, and simplified security software with automatic updates to reduce attack surface.

03

Establish Communication Protocols

Create family verification systems using code words or specific callback procedures for any financial requests claiming emergencies.

04

Enable Banking Protections

Set up transaction alerts, transfer limits, and trusted contact designations at financial institutions serving senior clients.

05

Foster Reporting Culture

Normalize discussing attempted scams to reduce stigma, encouraging seniors to report suspicious contacts without fear of judgment.

KEY TAKEAWAYS

Executive Summary & Action Items

Rising Threat

Senior-targeted cybercrime continues accelerating, with losses exceeding $3.4B annually. AI-enhanced attacks will intensify this trend in 2025.

Vulnerability Factors

Digital literacy gaps, social isolation, and accumulated assets create perfect conditions for exploitation through emotional manipulation.

Layered Defense

Protection requires coordinated education, technical controls, family involvement, financial safeguards, and accessible reporting systems.

Organizational Role

Security professionals must champion senior-specific protections, adapting enterprise security frameworks to address unique age-related vulnerabilities.

Organizations should audit current protections for senior stakeholders, implement targeted training programs, and establish partnerships with community organizations serving older adults.

About Cyber Security Non-Profit

Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety
- Senior Digital Safety
- Women's Security
- Parents & Educators

Everything we offer is free. Access training materials, guides, and community support at no cost.

Visit CSNP.org

Browse Resources