



ELIMINATING CYBERCRIME AND ARTIFICIAL INTELLIGENCE- DRIVEN FRAUD

— A WHITE PAPER AND SOLUTIONS PROJECT —

— CELEBRATING ALABAMA'S PROGRESS —
CERTIFIED PUBLIC MANAGERS® PROGRAM
— CPM SOLUTIONS ALABAMA 2026 —



TABLE OF CONTENTS

PROJECT TEAM	3
ACKNOWLEDGMENTS.....	4
PROJECT STATEMENT	5
INTRODUCTION: THE HUMAN IMPACT OF CYBERCRIME IN ALABAMA	6
A True Story: Adam’s Story.....	6
A True Story: When a Lifetime of Savings Disappears	8
A True Story: Fear in the Inbox.....	9
BACKGROUND	11
Understanding Today’s Cyber Threats: Key Terms and Common Fraud Schemes	12
Key Terms and Concepts	12
Common Fraud Schemes	14
The Changing Threat Landscape	16
ALABAMA’S CURRENT RESPONSE: Where We Are Today	19
ALABAMA’S CURRENT RESPONSE: Legislative Initiatives.....	22
COMPARATIVE ANALYSIS OF STATE BEST PRACTICES	23
Public Awareness and Consumer Education	24
Centralized Consumer Resources and Reporting.....	26
Standardized Cybersecurity Education	27
RECOMMENDATIONS.....	29
Establish a Statewide Fraud Awareness Campaign	30
Develop a Centralized Statewide Fraud Reporting and Resource Portal.....	32
Establish a Lifelong Fraud Prevention Education Program	35
CONCLUSION	39
APPENDICES	47

PROJECT TEAM

This project was developed through a collaborative effort by a diverse CPM Solutions Alabama Team dedicated to examining cybercrime, artificial intelligence-driven fraud, consumer protection, and practical strategies to strengthen Alabama’s response to emerging digital threats. The following individuals contributed research, analysis, recommendations, and project support:

Alabama Board of Examiners in Psychology

Lori Rall



Alabama Department of Corrections

Jeffrey Burt

Chitema Westry



Alabama Department of Environmental Management

Scott Jackson

James Worley



Alabama Public Service Commission

Kasey Hitson



Alabama Department of Revenue

Karl Gore



Alabama Department of Transportation

Ramy Abdalla



The research, analysis, and recommendations presented in this white paper do not necessarily represent the official views of any participating agency or organization. Rather, they reflect the collective work of the above participants as part of the Certified Public Manager® Program.

ACKNOWLEDGMENTS

The **Eliminating Cybercrime Solutions Alabama Project Team** extends its sincere appreciation to our stakeholder partner, the **Alabama Securities Commission**, whose leadership, expertise, and collaboration were instrumental in informing the research, analysis, and recommendations presented in this paper. We are especially grateful to the Commission's leadership and subject matter experts for generously sharing their time and knowledge throughout this project.

We also extend our heartfelt appreciation to **Adam and his family** for their willingness to share their personal experience. Their story served as a powerful reminder that behind every fraud statistic is a person whose experience can help educate and protect others.

We would especially like to recognize:

Amanda Senn

Director

Alabama Securities Commission

Steve Feaga

Chief Deputy

Alabama Securities Commission

Miles Faggart

Senior Special Agent

Alabama Securities Commission

Adam and His Family

For sharing their experience in support of public education and fraud prevention.



PROJECT STATEMENT

Cybercrime has rapidly evolved from a technical threat targeting computer systems into a broad challenge affecting public safety, economic security, and consumer protection. The rise of advanced artificial intelligence (AI) has accelerated this evolution, enabling criminals to exploit trust through highly convincing scams, impersonate trusted individuals, automate fraudulent communications, and target victims at an unprecedented scale. Throughout this paper, these evolving threats are collectively referred to as *cyber-enabled fraud*.

Across Alabama, citizens, businesses, and institutions now face increasing exposure to cyber-enabled fraud, including investment and romance scams, identity theft, business email compromise, cryptocurrency fraud, and AI-enabled scams. These crimes have become a pervasive threat to the state's residents, financial markets, and economic stability.

The Alabama Securities Commission (ASC) served as the primary stakeholder agency for this Certified Public Manager® (CPM) Solutions Alabama Project (the project). Throughout the project, ASC leadership and subject matter experts provided a series of briefings on emerging trends in cybercrime, AI, cryptocurrency, and investment fraud. These briefings provided the CPM Solutions Alabama Team with valuable context and informed research, analysis, and findings presented throughout this paper.

This project examines the escalating threat of cyber-enabled consumer and investment fraud involving cryptocurrency and AI in Alabama. Over the past decade, these crimes have increased dramatically, resulting in substantial financial losses and creating significant risks for investors, businesses, and consumers across the state.

To address these challenges, the project focused on four primary objectives:

1. Evaluate Alabama's current legislative, regulatory, and public awareness efforts to combat cybercrime and AI-driven fraud.
2. Compare Alabama's efforts with best practices implemented by California, Florida, Kentucky, New York, and Tennessee to identify effective statewide strategies.

3. Assess the characteristics, growth, and impact of cybercrime and AI-driven fraud affecting Alabama consumers.
4. Develop actionable statewide recommendations to strengthen Alabama's coordinated approach to prevention, education, enforcement, and consumer protection.

The research conducted through this project provides the foundation for actionable recommendations to strengthen Alabama's ability to prevent, detect, and respond to cyber-enabled financial fraud through coordinated legislation, effective regulation, public education and awareness, and collaboration among government, industry, and community stakeholders.

INTRODUCTION: THE HUMAN IMPACT OF CYBERCRIME IN ALABAMA

Cybercrime often sounds like some else's problem, described through technical terminology, cybersecurity frameworks, and statistics that can make the threat seem distant from everyday life. In reality, today's cybercriminals are far more likely to exploit human trust than computer vulnerabilities. A familiar voice on the telephone, a convincing text, or an email that appears to come from a trusted source can now be just as dangerous as a sophisticated computer attack.

Many damaging schemes exploit fear and trust, creating a sense of urgency that pressures victims into acting before they have time to think critically or investigate the situation (Federal Trade Commission [FTC], 2023). The victims are not abstract figures reflected in reports or statistics; they are Alabamians whose finances, relationships, and sense of security have been profoundly disrupted.

Three examples illustrate the changing nature of fraud.

A True Story: Adam's Story

The following account is based on an actual incident in Alabama. The individual's name and identifying details have been changed to protect his privacy. The account was shared with the CPM Solutions Alabama Team with permission for educational purposes.

In late summer following his high school graduation, Adam seemed prepared for a promising future. He had graduated near the top of his class, earned an athletic scholarship to a prestigious

private college in central Alabama, and spent years saving nearly \$10,000 to cover expenses not included in his scholarship. Known for his strong work ethic and good judgment, Adam had little reason to believe he would soon become the victim of a devastating cybercrime.

Shortly after moving into his college dorm, Adam began using social media more freely than he had while living at home. Within hours of creating an Instagram account, he received a message from someone posing as an attractive college student at a nearby university. What appeared to be a casual online conversation was, in reality, the opening move in a carefully orchestrated fraud scheme.

Conversation was friendly and flattering, quickly becoming personal during a time when Adam was adjusting to a new environment and eager to make friends. Over the next several hours, the scammer pieced together information from Adam's messages, publicly available social media profiles, and weak privacy settings. They learned about his family, friends, teammates, religious background, school history, and other personal details. Believing he was communicating with a genuine romantic interest, Adam eventually shared a suggestive photograph after receiving similar images and increasingly intimate messages.

The tone of the conversation changed immediately.

The scammer threatened to send Adam's photograph and message history to his parents, friends, teammates, classmates, and a young woman they knew was especially important to him. Panicked and embarrassed, Adam sent several hundred dollars through an online payment platform in exchange for the scammer's promise to delete the shared images and remain silent.

The payment did not end the threats.

Instead, it confirmed that Adam was frightened and willing to pay.

The scammer became increasingly aggressive, sending screenshots of Adam's social media accounts and identifying people by name. With each payment came another demand. In less than twenty-four hours, Adam emptied nearly all of his college savings account – money he had earned through years of part-time jobs and careful planning. Still, the threats continued.

Exhausted, frightened, and financially devastated, Adam finally told his parents. Convinced he had ruined his reputation and disappointed everyone he loved, he feared humiliation almost as much as financial loss. His parents immediately contacted law enforcement and campus security. Although investigators communicated directly with the overseas criminals responsible for the scheme, the stolen funds were never recovered. Adam's college savings were gone.

Adam's experience illustrates how quickly social engineering and sextortion can victimize even intelligent, responsible, and financially cautious young adults. He was neither reckless nor technologically incapable. He was inexperienced, trusting, and unaware of how quickly an online relationship could be weaponized. Earlier education regarding sextortion, privacy settings, account security, social engineering, and AI-enhanced impersonation might have helped him recognize the warning signs before the situation escalated. The consequences of these crimes extend far beyond financial loss and may include humiliation, emotional distress, damaged relationships, and a lasting loss of confidence.

Adam's experience is not unique.

The Montgomery County District Attorney (2022) warned that sextortion scams targeted numerous families with teenaged boys and that the crime had become an increasing concern locally. Many victims were so ashamed and frightened that they initially tried to handle the situation alone before finally confiding in a parent or another trusted adult. The district attorney explained that organized criminal groups operating outside the area, or even the United States, deliberately targeted adolescent boys because they believed they would be less likely to report the crime. The district attorney further warned that paying extortion demands never stopped the threats and urged victims to contact law enforcement immediately (Bowerman, 2022).

A True Story: When a Lifetime of Savings Disappears

Like many older adults, an Alabama woman had spent years carefully building her savings and planning for the future. She never imagined that a series of convincing conversations would place everything she had worked for at risk.

The scammers persuaded her that her savings were in immediate danger and that acting quickly was the only way to protect her money. Trusting the instructions she received, she withdrew cash from her accounts and deposited it into cryptocurrency ATMs. Once the funds were converted into digital currency, which happens quickly, they were transferred beyond her control and became virtually impossible to recover.

According to *WSFA 12 News*, the Huntsville, woman ultimately lost more than \$330,000 through the scheme. The finance and emotional impact was so devastating that Alabama lawmakers later cited her case when introducing legislation designed to strengthen consumer protections against cryptocurrency ATM fraud (Henry, 2026).

This experience illustrates how modern fraud schemes increasingly target older adults through carefully crafted and sophisticated social engineering tactics that exploit fear, trust, and urgency rather than technical expertise. It also demonstrates how quickly cyber-enabled financial exploitation can erase a lifetime of savings, underscoring the need for stronger consumer education, fraud prevention, and safeguards surrounding cryptocurrency transactions.

A True Story: Fear in the Inbox

One morning in September 2024, residents across Mobile opened their email to what appeared to be every person's worst nightmare.

The message claimed that a stranger had hacked the recipient's computer, secretly activated their webcam, and recorded intimate moments inside the victim's own home. To make the threat seem undeniable, the sender included passwords that many recipients recognized from years earlier in the message. Unless payment was made immediately in Bitcoin, the email warned that the alleged videos would be sent to family members, friends, and coworkers.

For many recipients, the fear was immediate.

The threat felt real. The threat felt personal. The passwords appeared authentic. The consequences described in the message were deeply embarrassing. For someone unfamiliar with how these scams operate, the email seemed entirely believable.

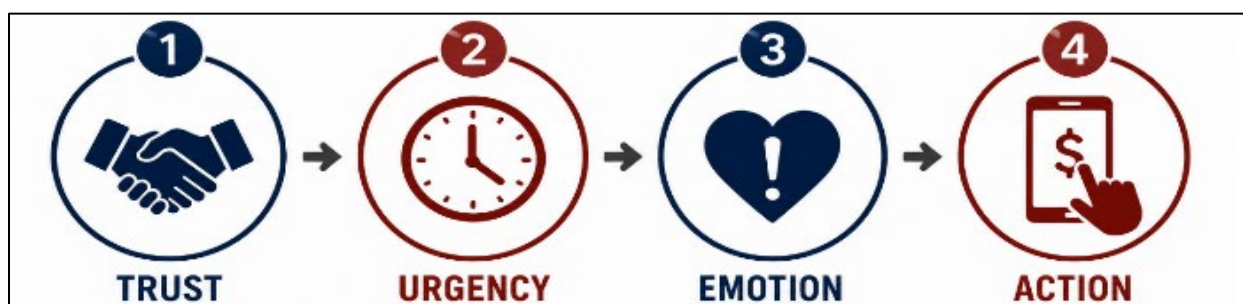
According to the Mobile Police Department, however, the messages were nothing more than a sophisticated and elaborate cryptocurrency extortion scheme. The scammers had not secretly recorded their victims. Instead, they relied on passwords stolen during previous data breaches and carefully crafted messages designed to create panic, urgency, and shame. Their greatest weapon was not malicious software. It was fear.

Investigators urged residents not to pay the extortion demands and instead report the incident to law enforcement. The case demonstrates how modern cybercriminals increasingly exploit human emotion rather than technical vulnerabilities and how quickly a convincing message scam can succeed to overwhelm otherwise careful decision-making (Fox10TV, 2024).

A Common Pattern: Trust, Urgency, Emotion, Action

Although the victims, circumstance, and methods differ, the underlying strategy remains remarkably consistent. These examples reveal a consistent pattern: cybercriminals establish trust, create urgency, exploit emotion, and pressure victims to act before they have time to verify the situation or think critically.

Cybercrime is no longer a threat confined to technology professionals or large organizations. It affects every Alabama resident who uses a telephone, email account, bank account, social media platform, or other digital services.



Modern fraud increasingly uses psychological manipulation and deceptive appearances to exploit victims across age groups, particularly through investment fraud and confidence/romance schemes (Federal Bureau of Investigation [FBI], 2026). As these schemes continue to evolve, understanding how they work is just as important as recognizing the technologies that enable

them. This growing vulnerability underscores the need for stronger public education, greater awareness, and coordinated efforts to prevent fraud before it occurs.

BACKGROUND

Alabama, like the rest of the nation, faces an evolving cybercrime and fraud landscape characterized by substantial financial losses, increasingly sophisticated scams, and the growing use of emerging technologies such as artificial intelligence. Criminals increasingly exploit digital communication channels, including text messages, social media, online advertisements, dating applications, and messaging platforms, to obtain personal and financial information and manipulate victims through sophisticated fraud and social engineering techniques (FBI, 2026).

The emergence of generative artificial intelligence has further expanded the methods available to malicious actors and introduced new risks to individuals and organizations. Generative AI can lower barriers to offensive cyber capabilities by facilitating activities such as hacking, malware, phishing, vulnerability exploitation, and other cyberattacks. It can also increase the ease and scale with which deceptive or misleading content is created, providing malicious actors with additional tools to support increasingly sophisticated cyber-enabled schemes (National Institute of Standards and Technology [NIST], 2024).

These evolving threats affect a broad range of potential victims. Alabama's diverse population, including older adults and residents across other age groups and communities, faces a fraud environment characterized by increasingly sophisticated schemes and substantial financial losses. Consumers are affected by fraud involving investment schemes, impersonation, identity theft, and other forms of technology-enabled deception, while email, telephone calls, and text messages remain common methods used by scammers to contact potential victims (FBI, 2026; Federal Trade Commission [FTC], 2025b). The widespread and evolving nature of these threats demonstrates the importance of coordinated prevention, consumer education, reporting, and response strategies to reduce financial losses and strengthen public resilience.

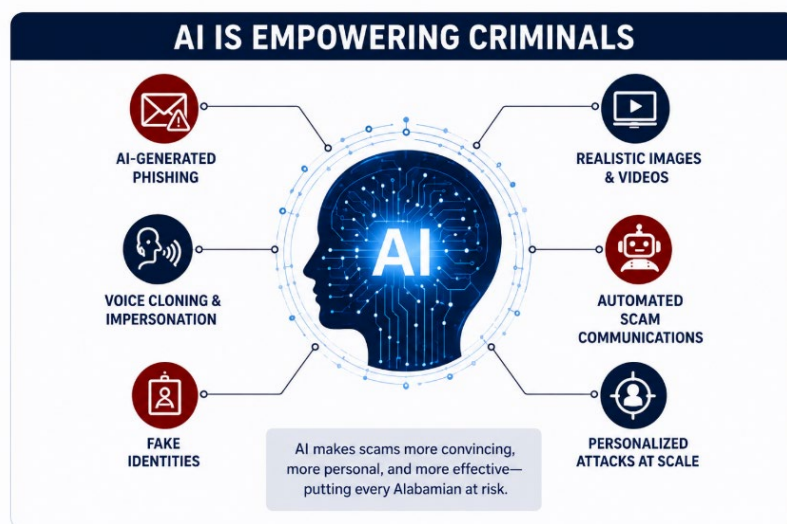
During discussions with ASC representatives, the agency reported a significant rise in investment fraud, romance-linked financial exploitation, cryptocurrency-related scams, and AI-generated

impersonation schemes (Alabama Securities Commission, personal communication, 2026). These trends mirror national patterns identified by federal law enforcement and consumer protection agencies but also highlight the need for a tailored statewide approach that strengthens public awareness, enhances digital literacy, and improves collaboration among government agencies, financial institutions, educational organizations, and community partners (FBI, 2026).

This evolving threat landscape underscores the urgency of developing a proactive statewide strategy that prepares Alabama residents, institutions, and public agencies to recognize, prevent, and respond to cyber-enabled fraud. Because cybercrime encompasses a rapidly expanding array of technologies, tactics, and fraud schemes, understanding the terminology used throughout this report provides an essential foundation for the research, findings, and recommendations that follow.

Understanding Today's Cyber Threats: Key Terms and Common Fraud Schemes

Cybercrime and AI continue to reshape the methods criminals use to commit financial fraud. Rather than relying solely on technical expertise, today's criminals increasingly combine technology with psychological manipulation to make scams more convincing, automate fraudulent activities, and reach



more victims than ever before. Understanding the following key terms and common fraud schemes provides a foundation for recognizing these evolving threats and for understanding the research, findings, and recommendations that follow.

Key Terms and Concepts

Artificial Intelligence (AI): Computer systems capable of performing tasks that typically require human intelligence, including learning, reasoning, recognizing patterns, solving problems, and

generating content. Although AI has many beneficial applications, it can also be exploited by criminals to make fraud schemes more sophisticated, scalable, and convincing (National Institute of Standards and Technology [NIST], 2023).

Generative AI: A type of AI capable of creating original text, images, audio, video, and computer code. Criminals increasingly use generative AI to produce realistic phishing emails, fraudulent websites, voice clones, and deepfake videos designed to deceive victims and facilitate cyber-enabled fraud (NIST, 2023).

AI-Driven Fraud: Fraud schemes in which criminals use artificial intelligence to enhance, personalize, or automate traditional scams. Common examples include voice cloning, deepfake impersonations, AI-generated phishing emails, fraudulent investment solicitations, and automated online scams that appear legitimate (FBI, 2026; NIST, 2023).

Deepfake: AI-generated or AI-manipulated audio, video, or images, or other digital content designed to realistically imitate the appearance, voice, or actions of another person. Criminals use deepfakes to impersonate family members, business executives, celebrities, or public officials, and other trusted individuals to facilitate fraud and other forms of deception (Cybersecurity and Infrastructure Security Agency [CISA], n.d.-a).

Cybercrime: Criminal activity involving computers, digital devices, networks, or the internet as target, tool, or means of committing an offense (National Institute of Standards and Technology [NIST], n.d.). Common examples include identity theft, ransomware attacks, financial fraud, online scams, and unauthorized access to computer systems.

Social Engineering: A form of psychological manipulation in which criminals exploit trust, fear, urgency, or other emotions to persuade victims to reveal sensitive information, transfer money, or take actions that benefit the attacker. Rather than exploiting computer systems, social engineering targets human behavior (CISA, n.d.-a).

Digital Literacy: The ability to use digital technologies safely, effectively, and responsibly while recognizing online risks, evaluating information, and protecting personal information. Strong

digital literacy includes cybersecurity awareness and helps individuals recognize threats such as phishing, safeguard personal data, and make informed decisions when using digital technologies (Team CommUNITY, n.d.).

Cybersecurity: The practice of protecting computers, networks, digital devices, and information from unauthorized access, theft, disruption, or damage. Effective cybersecurity combines technology, sound policies, and informed users to reduce cyber risks and strengthen resilience against evolving threats (NIST, n.d.).

Multi-Factor Authentication (MFA): A security measure requiring two or more forms of identity verification before granting access to an account or system. Common forms include a password combined with a verification code, biometric scan and authentication, or an authentication application. MFA significantly reduces the risk of unauthorized account access, even when passwords have been compromised (CISA, n.d.-b).

Common Fraud Schemes

The methods criminals use continue to evolve, but their objective remains remarkably consistent: exploiting human trust for financial gain. Today, cybercriminals combine traditional confidence schemes with modern technology, cryptocurrency, and AI to carry out increasingly sophisticated fraud. The following examples illustrate some of the most common cyber-enabled threats affecting consumers today.

Phishing, Smishing, and Vishing: Fraud schemes that attempt to steal sensitive information, gain unauthorized access to accounts, or obtain money through email (phishing), text messages (smishing), or telephone calls (vishing). Advances in AI have made these attacks increasingly convincing through realistic emails, text messages, voice cloning, and other forms of personalized communication (CISA, 2024).

Government Imposter Scam: Fraud schemes in which criminals falsely claim to represent a government agency or employee to obtain personal information or money from victims. Scammers may use threats, demands for payment, or other deceptive tactics and may contact

victims by telephone, email, text message, social media, or mail (Alabama Securities Commission [ASC], 2024); National Security Agency Office of the Inspector General [NSA OIG], 2022).

Romance Scam: A fraud scheme in which criminals create fictitious romantic relationships through dating websites, social media platforms, or messaging applications to gain a victim's trust. Once an emotional connection has been established, criminals request money for emergencies, travel expenses, medical bills, or fraudulent investment opportunities, often escalating their demands over time (ASC, 2024).

Pig Butchering Scam: A long-term investment fraud in which criminals establish and cultivate a relationship with a victim, gradually earning the victim's trust before encouraging increasingly larger investments into fraudulent cryptocurrency or other investment platforms. The scheme is referred to by law enforcement and cybersecurity organizations as "pig butchering" because victims are persuaded to invest retirement savings, life savings, or borrowed funds over time, a process described as "fattening the pig". Once the victim has invested as much as possible, the criminals disappear with the money, an outcome referred to as the "pig is butchered" (ASC, 2024; Federal Bureau of Investigation [FBI], n.d.-b).

Investment Fraud: Fraud involving false or misleading investment opportunities designed to obtain money through deception. Common examples include Ponzi schemes, affinity fraud, promissory note fraud, fraudulent cryptocurrency investment platforms, and promises of guaranteed returns with little or no investment risk. These schemes often exploit trust, financial goals, or fears of missing investment opportunities to persuade victims to invest increasing amounts of money (ASC, 2023a).

Cryptocurrency Fraud: Cryptocurrency fraud occurs when scammers use digital currencies, such as Bitcoin or Ether, to deceive individuals into sending money or making fraudulent investments. Cryptocurrency is particularly attractive to scammers because payments are typically irreversible and may offer fewer protections than traditional payment methods (Federal Trade Commission [FTC], 2022).

Elder Financial Exploitation: The illegal or improper use of an older adult's money, property, or assets through deception, coercion, undue influence, or abuse of trust. Older adults are generally

considered to be individuals 60 years of age or older. Criminals commonly pose as financial advisors, caregivers, government officials, technical support representatives, or even family members to gain access to a victim's finances (ASC, 2023b).

Business Email Compromise (BEC): A fraud scheme in which criminals impersonate executives, employees, trusted vendors, or other business contacts to persuade organizations to transfer money or disclose sensitive financial or business information. These attacks commonly target payroll systems, wire transfers, and vendor payments, accounts payable processes, and vendor payment requests, often by creating a false sense of urgency or authority (Federal Bureau of Investigation [FBI], n.d.-a).

Ransomware: Malicious software that encrypts or blocks access to a victim's computer system or files or files until a ransom is paid, often in cryptocurrency. Even after payment, there is no guarantee that access will be restored, stolen information will remain private, or future extortion attempts will not occur (CISA, n.d.-a).

Clipboard Hijacking: A type of malware that monitors a user's computer clipboard for copied cryptocurrency wallet addresses. The malware secretly replaces the legitimate wallet address with one controlled by the attacker, causing cryptocurrency intended for the legitimate recipient to be transferred to the criminal instead. Because the substitution occurs invisibly, victims often do not realize the wallet address has been altered until the transaction is complete and the funds cannot be recovered (Consensys, 2026).

QR Code Fraud (Quishing): Also known as "quishing," this fraud scheme uses fraudulent QR codes to direct victims to counterfeit websites or payment portals designed to steal login credentials, personal information, or money. Because QR codes conceal the destination website until they are scanned, victims may unknowingly visit malicious sites that appear legitimate (United States Postal Inspection Service [USPIS], 2025).

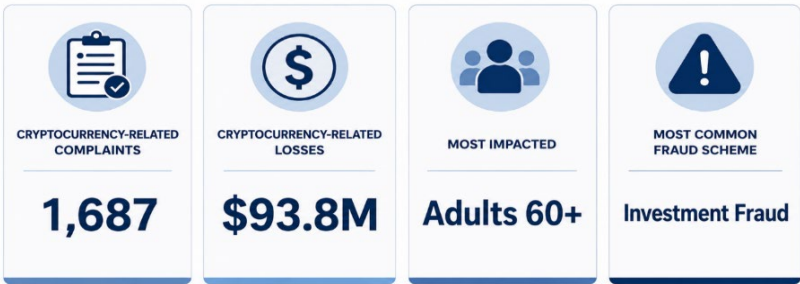
The Changing Threat Landscape

AI is transforming the speed, scale, and sophistication of fraud across Alabama. Criminals now use AI to craft highly convincing phishing messages, clone voices, generate fake identities,

produce realistic images and videos, automate scam communications, and tailor attacks to individual victims.

As a result, traditional fraud schemes are becoming more effective as AI enables criminals to appear more credible and human. The challenge facing Alabama is no longer limited to technical cybersecurity concerns; it is the broader protection of citizens, financial systems, and public trust.

ALABAMA’S CURRENT STATISTICS: Cybercrime Snapshot

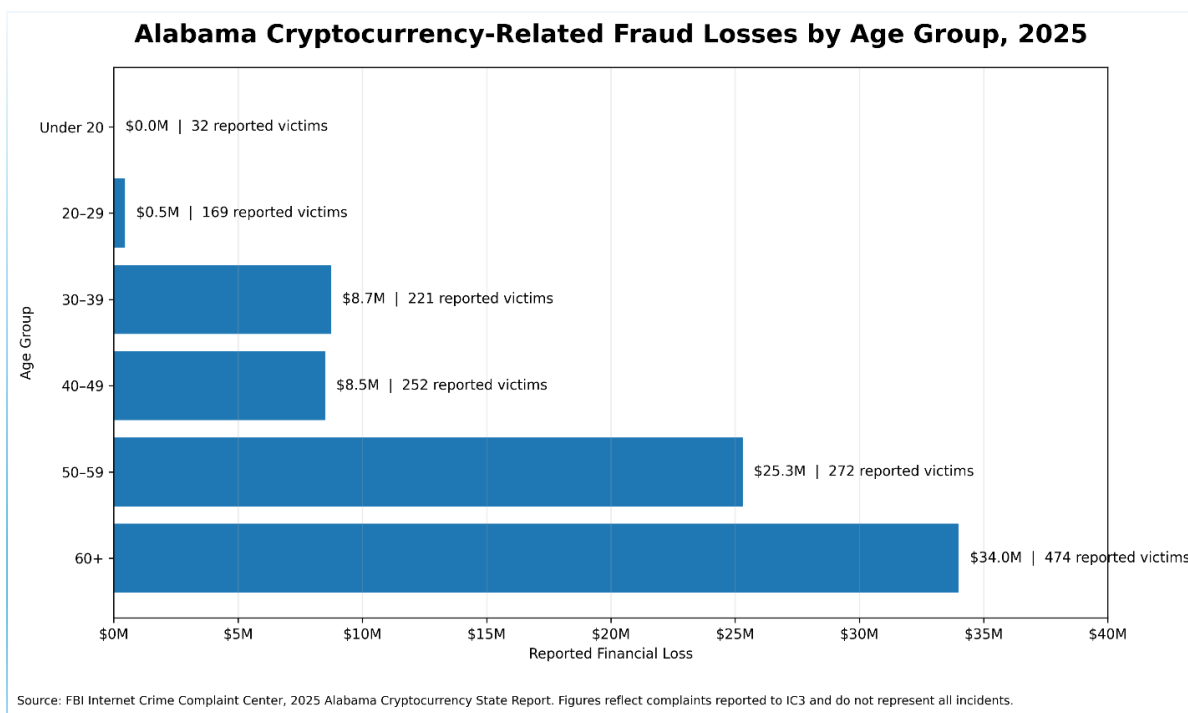


Source: Federal Bureau of Investigation (FBI), Internet Crime Complaint Center (IC3), 2026.

Cybercrime and cryptocurrency-related fraud continue to impose substantial financial losses on individuals across the United States and in Alabama.

According to the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3), 181,565 cryptocurrency-related complaints were reported nationwide during 2025, resulting in more than \$11.3 billion in reported losses. During the same period, IC3 received 1,687 cryptocurrency-related complaints from Alabama, totaling more than \$93.8 million in reported losses (FBI, 2026). The FBI identified investment fraud as the most commonly reported form of cryptocurrency-related fraud, illustrating the continued prevalence of scams involving fraudulent investment opportunities (FBI, 2026).

Although cybercrime affects individuals of all ages and backgrounds, its financial impact is not distributed equally. Adults 60 years of age and older continue to experience the greatest financial losses from cryptocurrency-related fraud (FBI, 2026). Earlier Alabama data similarly identified older adults as demographic experiencing the greatest financial losses, followed by individuals 50 to 59 years of age, suggesting that criminals frequently target those with greater accumulated savings or retirement assets (FBI, 2024). However, these scams are not limited to older adults. The Federal Trade Commission (FTC) reports that investment scams generate the highest financial losses nationwide, demonstrating that financially established individuals who actively make investment decisions are also frequent targets (Federal Trade Commission [FTC], 2025a).



Reported cryptocurrency-related financial losses increased substantially among older age groups, with Alabamians aged 60 and older experiencing the highest total losses. Figures reflect complaints submitted to the FBI’s Internet Crime Complaint Center and may not represent all incidents (FBI, 2026).

While detailed county-level reporting remains limited, available information indicates that cryptocurrency-related fraud is concentrated in Alabama's more populous communities, including Jefferson County, Montgomery, Huntsville, and Mobile. These areas have experienced increasing reports of cryptocurrency ATM scams and investment fraud, likely reflecting larger populations, greater financial activity, and broader access to and use of digital financial services (Schuessler, 2025). Although Alabama reports fewer overall victims than many larger states, it has consistently ranked among the highest in financial losses per victim, underscoring the importance of strengthening fraud prevention, public education, and consumer awareness throughout the state (FBI, 2026). Although these statistics are derived primarily from federal reporting rather than Alabama-specific reporting systems, they illustrate the significant impact of cybercrime on Alabama residents. The limited availability of detailed state-level data further highlights the need

for improved fraud reporting and data collection in order to better identify emerging trends, target prevention efforts, and inform future policy decisions.

ALABAMA'S CURRENT RESPONSE: Where We Are Today

Alabama addresses cybercrime and AI-enabled fraud through the combined efforts of multiple state agencies, financial institutions, educational organizations, and local community partners. These organizations provide consumer education, cybersecurity awareness, victim resources, complaint reporting, and fraud prevention initiatives through their respective missions. While these efforts demonstrate Alabama's strong commitment to addressing emerging cyber threats, they are administered independently rather than through a single coordinated statewide strategy.

ASC serves as one of the state's primary resources for investor protection, consumer fraud education, and securities-related complaint reporting. Through its Financial Exploitation Division, the ASC publishes newsletters and consumer alerts addressing common fraud schemes, including account takeover fraud, financial institution impersonation scams, money mule schemes, investment fraud, and family financial exploitation (Alabama Securities Commission [ASC], n.d.). The Commission also administers the She Can financial empowerment initiative, which provides educational content through social media, podcasts, and community outreach to help consumers recognize financial scams and make informed financial decisions (ASC, 2026a). In addition to these educational efforts, the ASC maintains an online complaint process for consumers to report suspected securities fraud and financial exploitation. The Commission publishes annual agency statistics summarizing complaints, enforcement actions, investor education activities, and restitution obtained for victims. During Fiscal Year 2023–2024, the ASC reported 221 complaints and corporate inquiries, 166 investor education and fraud prevention events, and \$891,411 in restitution ordered to victims (Alabama Securities Commission [ASC], 2025). These statistics provide valuable insight into the Commission's work; however, they are limited to matters within the ASC's jurisdiction and therefore do not provide a comprehensive statewide picture of cybercrime or fraud affecting Alabama residents.

Additional educational resources are provided by a variety of state agencies, higher education institutions, nonprofit organizations, and local community organizations. The Alabama Office of

Information Technology (OIT) maintains cybersecurity information for Alabama citizens and directs users to online safety, cyber incident reporting, and other cybersecurity resources (Alabama Office of Information Technology, 2026). Universities, public libraries, and regional organizations also provide cybersecurity workshops, fraud awareness presentations, and community education opportunities. The University of South Alabama promotes cybersecurity awareness through its CyberSmart initiative, Homewood Public Library has offered cybersecurity workshops addressing phishing, password security, and safe browsing practices, and SARCOA provides fraud-prevention education for older adults through events such as its Fraud Summit (SARCOA, 2026; The Homewood Star, 2026; University of South Alabama, 2025). Although these programs provide valuable educational opportunities, their availability, subject matter, and intended audiences vary across sponsoring organizations in the state.

The State has also invested in expanding digital access through several statewide initiatives. The Alabama Digital Opportunity Plan focuses on expanding digital access and developing the skills necessary for residents to participate effectively in an increasingly connected environment (Alabama Department of Economic and Community Affairs [ADECA], 2024a). In addition, the Broadband Equity, Access, and Deployment (BEAD) Program focuses on expanding broadband infrastructure and improving access to reliable, high-speed internet throughout the state (ADECA, 2024b). Together, these initiatives address barriers to digital participation, particularly among underserved populations and communities. While these efforts improve residents' ability to access and navigate online services, cybersecurity awareness and fraud prevention are incorporated within broader digital literacy efforts rather than serving as the primary focus of the programs (ADECA, 2024a). Separately, the Alabama Office of Information Technology provides cybersecurity awareness, education, and online safety resources for Alabama citizens (Alabama Office of Information Technology [OIT], 2026). Alabama therefore supports cybersecurity awareness and fraud prevention through existing state agency programs and broader digital literacy initiatives; however, publicly available state program documentation does not identify a dedicated statewide funding program specifically focused on consumer cyber fraud prevention and education.

Financial institutions also play an important role in educating consumers about fraud prevention. According to the Alabama State Banking Department (Banking), 88 state-chartered commercial banks operated within Alabama during Fiscal Year 2025 (Alabama State Banking Department, 2026). Research conducted for this project included outreach to five state-chartered banks to determine whether fraud prevention education is provided during the account-opening process. Responses revealed considerable variation among institutions. West Alabama Bank reported providing customers with brochures describing common fraud indicators and reviewing applicants' credit histories as part of its account-opening process. First Bank of Alabama indicated that financial literacy resources are available through its website but are generally provided only upon customer request. Other institutions either declined to provide information or referred inquiries to other departments. These findings suggest that fraud prevention education is largely determined by the practices of individual financial institutions rather than a consistent or standardized statewide approach.

Cybercrime and fraud reporting within Alabama occurs through multiple state and federal reporting channels rather than a single reporting mechanism. Depending on the nature of the incident, consumers may submit complaints involving securities or investment-related fraud to the Alabama Securities Commission (Alabama Securities Commission, 2026a), while the Alabama Office of Information Technology (OIT) provides resources for reporting cyber incidents and accessing cybersecurity guidance (Alabama Office of Information Technology [OIT], 2026). At the federal level, consumers may report internet-facilitated crime to the FBI's Internet Crime Complaint Center (IC3) (FBI, n.d.-c) or cyber incidents through the Cybersecurity and Infrastructure Security Agency's incident reporting system (Cybersecurity and Infrastructure Security Agency [CISA], 2026). These reporting mechanisms provide valuable services within their respective jurisdictions; however, the publicly available resources reviewed do not identify a centralized Alabama reporting portal or public dashboard that consolidates complaint information across these agencies. As a result, available reporting mechanisms may limit the State's ability to aggregate cross-agency complaint data, identify comprehensive statewide fraud trends, and support coordinated public reporting and policy analysis.

Collectively, Alabama's current efforts demonstrate a strong commitment to cybersecurity awareness, investor protection, and fraud prevention. State agencies, financial institutions, educational organizations, and community partners each contribute valuable educational resources, complaint reporting mechanisms, and outreach initiatives. A review of publicly available state program and reporting resources shows that these functions are distributed across separate agencies and programs, including ADECA's digital literacy initiatives, OIT's cybersecurity resources, and ASC's fraud prevention and complaint reporting activities, rather than consolidated within a single statewide framework (ADECA, 2024a; OIT, 2026; ASC, 2026a). As cyber-enabled fraud continues to evolve, this decentralized approach presents opportunities to strengthen statewide coordination, improve public access to reporting resources, enhance data sharing, and better inform consumer education, fraud trend analysis, and future policy decisions.

ALABAMA'S CURRENT RESPONSE: Legislative Initiatives

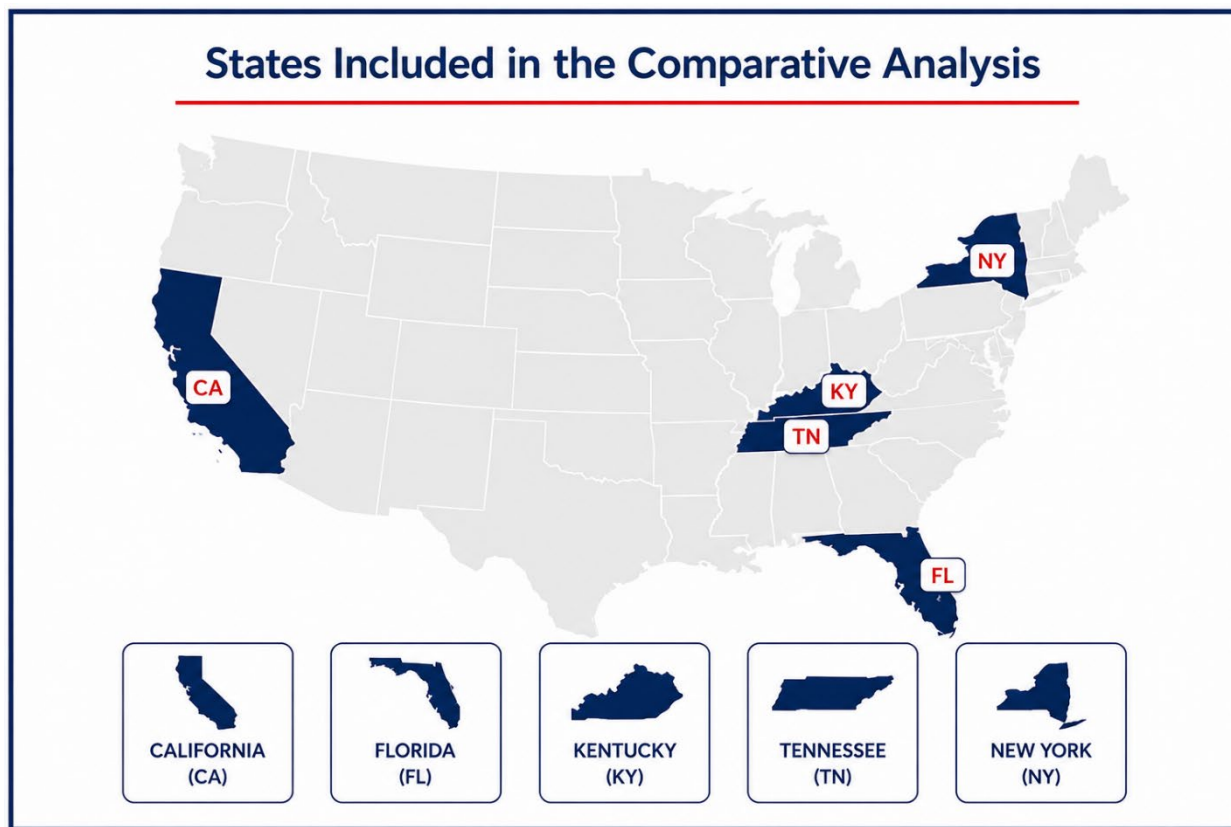
Alabama has recently enacted significant legislation to strengthen consumer protections related to cryptocurrency and other emerging digital financial technologies. During the 2026 Regular Session, the Alabama Legislature enacted House Bill 303, the Cryptocurrency Kiosk Fraud Prevention Act, and House Bill 259, the Financial Innovation and Market Expansion Act. Both laws become effective on October 1, 2026, reflecting Alabama's commitment to modernize its regulatory framework in response to the rapidly evolving digital financial landscape.

The Cryptocurrency Kiosk Fraud Prevention Act establishes comprehensive consumer protection requirements for cryptocurrency kiosk operators throughout Alabama. The Act establishes transaction limits for new and existing consumers, mandatory fraud warnings, clear disclosure of fees and exchange rates, identity verification, blockchain analytics to detect potentially fraudulent transactions, and 24-hour U.S.-based customer support. The Act also authorizes ASC to oversee compliance, investigate violations, and enforce the law through civil and criminal penalties. Additionally, eligible consumers who are induced to complete fraudulent cryptocurrency transactions may qualify for refunds if the fraud is reported within the statutory timeframe (Cryptocurrency Kiosk Fraud Prevention Act, 2026).

The Financial Innovation and Market Expansion Act establishes Alabama's regulatory framework for payment stablecoins and authorizes ASC to license and supervise qualified payment stablecoin issuers. The Act aligns Alabama's regulatory authority with the federal Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act and provides a statutory framework for implementing federal requirements and regulations governing payment stablecoins (ASC, 2026c; Financial Innovation and Market Expansion Act, 2026).

Because both legislative measures become effective on October 1, 2026, their long-term impact on consumer protection and fraud prevention has not yet been evaluated. Together, these laws establish the foundation of Alabama's current legislative framework for regulating cryptocurrency and other emerging digital financial technologies while demonstrating the State's commitment to strengthening consumer protections as these markets continue to evolve.

COMPARATIVE ANALYSIS OF STATE BEST PRACTICES



To identify effective strategies for reducing AI-driven fraud and cryptocurrency-related financial crimes, the project team conducted a comparative analysis of initiatives implemented in California, Florida, Kentucky, New York, and Tennessee. California and New York were selected because they are widely recognized as national leaders in cybersecurity, digital asset regulation, and consumer protection. Florida, Tennessee, and Kentucky were selected because they share demographic, economic, and governmental characteristics more comparable to Alabama while participating in many of the same federal partnerships and cybersecurity resources.

Rather than seeking a single model for Alabama to replicate, the analysis focused on identifying effective practices that appeared consistently across multiple states. Three common themes emerged: coordinated public awareness campaigns, centralized consumer resources, and cybersecurity education delivered through partnerships among schools, financial institutions, nonprofit organizations, and community groups.

Public Awareness and Consumer Education

One of the most consistent practices observed among the comparison states is the use of coordinated public awareness campaigns to keep residents informed about cyber threats and financial fraud. Rather than relying on a single communication method, these states distribute fraud prevention information through centralized websites, social media, scam alerts, public service announcements, and partnerships with local organizations.

Several states have established recognizable statewide initiatives that provide residents with trusted sources of cybersecurity

and fraud-prevention information. Tennessee's #CyberSafeTN, Florida's Secure Florida, and Kentucky's Stop Scams provide residents with educational resources, alerts, prevention guidance,



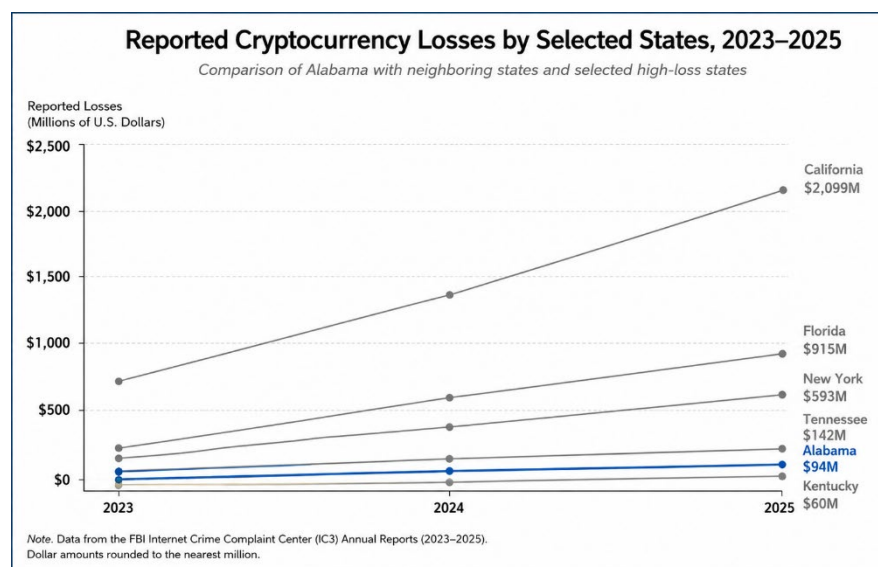
and information addressing cybersecurity threats, online scams, identity theft, and other forms of technology-enabled fraud (Florida Department of Law Enforcement, n.d.; State of Tennessee, n.d.-b; Team Kentucky, n.d.).

Digital communication further strengthens these outreach efforts. Tennessee distributes cybersecurity advisories, scam alerts, threat information, and educational resources through the Tennessee Cyber Hub and its #CyberSafeTN initiative (State of Tennessee, n.d.-b). New York similarly uses multiple state agencies to issue consumer alerts and guidance addressing emerging threats, including AI-generated fraud, identity theft, online scams, and other forms of technology-enabled fraud (New York Department of State, 2025; New York State Office of the Attorney General, 2024). Florida provides online cybersecurity guidance, best practices, and scam alerts to residents through Cyber Florida's Safer Connecting initiative (Florida Center for Cybersecurity, n.d.-b).

Several states further expand public awareness and cybersecurity preparedness through partnerships with community and private-sector organizations. California's Cybersecurity Integration Center (Cal-CSIC) coordinates cybersecurity information sharing among government agencies, utilities and service providers, academic institutions, nongovernmental organizations, and private-sector partners (California Governor's Office of Emergency Services, n.d.). Outside of state government, organizations such as Cyber-Seniors demonstrate how targeted outreach can provide cybersecurity and fraud-prevention education to older adults (Cyber-Seniors, n.d.). Florida and Kentucky similarly strengthen cybersecurity preparedness through partnerships involving law enforcement agencies, state and local governments, private-sector organizations, and other community and security partners (Florida Center for Cybersecurity, n.d.-a; Kentucky Office of Homeland Security, n.d.-b).

Although administered through different organizational structures, the comparison states consistently rely on coordinated public awareness campaigns, digital communication platforms, and community partnerships to provide residents with timely information about evolving cyber threats and financial fraud.

Centralized Consumer Resources and Reporting



In addition to public awareness campaigns, the comparison states provide centralized resources that help residents access cybersecurity information, identify appropriate reporting mechanisms, and obtain assistance following suspected fraud.

Although organizational structures differ, each state provides clearly identifiable resources where consumers can obtain trusted information and reporting guidance.

Tennessee's Cyber Hub and California's Cal-CSIC provide comprehensive statewide cybersecurity resource centers that consolidate educational materials, best practices, reporting guidance, and direct links to federal partners such as the CISA, the FBI, and the Internet Crime Complaint Center (IC3). California additionally uses Cal-CSIC to coordinate cybersecurity information among state agencies, local governments, law enforcement, educational institutions, and private-sector partners (California Governor's Office of Emergency Services, 2026.; State of Tennessee, n.d.-b).

Florida's Secure Florida and Kentucky's Stop Scams KY focus primarily on consumer assistance by combining fraud prevention information with reporting guidance, scam alerts, and victim resources. Although narrower in scope than Tennessee's Cyber Hub and California's Cal-CSIC, these initiatives provide residents with centralized locations to obtain assistance and report suspected fraud (Florida Department of Law Enforcement, n.d.; Team Kentucky, n.d.).

New York provides similar resources through multiple agencies rather than a single statewide portal. The Division of Consumer Protection provides consumer complaint and scam-reporting resources and publishes alerts addressing emerging threats, including AI-generated fraud and online scams (New York Department of State, n.d.-b). The Department of Financial Services

provides guidance on recognizing and reporting scams, fraud, cybercrime, and identity theft (New York State Department of Financial Services, n.d.). The Office of the Attorney General provides complaint-reporting resources for consumer, technology, privacy, investment, and financial issues and publishes consumer guidance addressing identity theft and other forms of fraud (New York State Office of the Attorney General, n.d.).

Although organizational structures differ, each comparison state provides readily accessible online resources that help residents obtain cybersecurity information, identify appropriate reporting mechanisms, and access government assistance following cybercrime or financial fraud.

Standardized Cybersecurity Education

While public awareness campaigns help residents recognize emerging cyber threats, many states have also invested in long-term educational initiatives that strengthen digital literacy and fraud prevention skills. Across the comparison states, cybersecurity education is delivered through partnerships with schools, higher education institutions, financial organizations, nonprofit agencies, and community groups.

Several states have integrated digital citizenship and cybersecurity education into K–12 schools and higher education. Kentucky incorporates digital citizenship into its K–12 educational framework, including digital security, privacy, responsible technology use, and other elements of digital citizenship (Kentucky Department of Education, 2025). Tennessee provides students with access to cybersecurity education and workforce-development resources, including information on university cybersecurity courses, degree programs, student cyber organizations, scholarships, internships, and other training opportunities (State of Tennessee, n.d.-a). National programs such as GenCyber and CyberPatriot further provide students with cybersecurity education and hands-on learning opportunities (CyberPatriot, n.d.; Department of Defense Cyber Exchange, n.d.).

Beyond formal education, several states provide cybersecurity and fraud-prevention education to adults through statewide programs, consumer-protection agencies, and community outreach. Florida's Secure Florida initiative promotes cybersecurity awareness and provides educational resources and outreach to help residents, businesses, and organizations better understand and

respond to cyber threats (Florida Department of Law Enforcement, n.d.). New York's Division of Consumer Protection provides educational materials, live outreach presentations, workshops, and scam-prevention resources to consumers and community organizations throughout the state (New York Department of State, n.d.-a). Kentucky similarly provides cybersecurity training and events that bring together government and cybersecurity professionals for education, hands-on training, information sharing, and collaboration (Kentucky Office of Homeland Security, n.d.-a).

Several comparison states provide educational initiatives tailored to older adults, who are frequently targeted by financial fraud and scams. California supports targeted technology and digital literacy education for older adults through state-funded Cyber-Seniors programs, including Connected Communities projects that provide technology training and support to older Californians (California Public Utilities Commission, 2026). New York's Division of Consumer Protection provides targeted fraud-prevention education through its Senior Anti-Fraud Education (S.A.F.E.) initiative, which helps older adults recognize common scams and provides guidance on protecting personal and financial information (New York Department of State, 2023).

The comparison states consistently demonstrates that cybersecurity education is strengthened when delivered through multiple partners rather than government agencies alone. Schools, colleges and universities, financial institutions, nonprofit organizations, and community groups each play complementary roles in strengthening digital literacy and fraud prevention knowledge across diverse populations.

Recurring Best Practices Across Comparative Analysis

BEST PRACTICE		REPRESENTATIVE STATE PROGRAMS				
	PUBLIC AWARENESS					
		CyberSafeTN	Secure Florida	Stop Scams KY	Cal-CSIC Outreach	Consumer Scam Alerts
						
		Tennessee Cyber Hub	SafeTN App	Secure Florida	Stop Scams KY	Cal-CSIC
						
		Digital Citizenship Standards	GenCyber	CyberPatriot	Cyber-Seniors	Senior Financial Education
	CENTRALIZED CONSUMER RESOURCES					
		Tennessee Cyber Hub	SafeTN App	Secure Florida	Stop Scams KY	Cal-CSIC
						
		Digital Citizenship Standards	GenCyber	CyberPatriot	Cyber-Seniors	Senior Financial Education
						
		Digital Citizenship Standards	GenCyber	CyberPatriot	Cyber-Seniors	Senior Financial Education
	CYBERSECURITY EDUCATION					
		Digital Citizenship Standards	GenCyber	CyberPatriot	Cyber-Seniors	Senior Financial Education
						
		Digital Citizenship Standards	GenCyber	CyberPatriot	Cyber-Seniors	Senior Financial Education
						
		Digital Citizenship Standards	GenCyber	CyberPatriot	Cyber-Seniors	Senior Financial Education

Although implemented through different organizational structures, the comparison states consistently emphasize coordinated public awareness, centralized consumer resources, and sustained cybersecurity education. These recurring practices provide a practical framework for strengthening Alabama's existing efforts.

*A visual summary of the states examined and the key practices informing this project is provided in **Appendix A, Learning from Leading States**.*

RECOMMENDATIONS

The comparative analysis identified several recurring best practices that were consistently implemented across the comparison states to strengthen cybersecurity awareness, fraud prevention, consumer protection, and interagency collaboration. Although each state employed a different organizational structure, common themes emerged throughout the research, including coordinated public awareness campaigns, centralized reporting and consumer resources, and standardized fraud prevention education delivered through partnerships among government agencies, educational institutions, financial organizations, and nonprofit organizations, and

community groups. These recurring strategies demonstrate that effective fraud prevention extends beyond law enforcement and requires a coordinated, statewide approach that emphasizes prevention, education, reporting, and collaboration.

Based on these findings, the following recommendations are intended to strengthen Alabama's ability to prevent, detect, and respond to cyber-enabled financial fraud, particularly investment and cryptocurrency-related scams. Collectively, they establish a comprehensive framework that expands public awareness, strengthens access to centralized reporting and consumer resources, and promotes lifelong fraud prevention education through trusted community partners. Together, these recommendations shift Alabama's approach from reacting to fraud after financial losses occur to building a coordinated statewide system that helps prevent fraud before residents become victims.

Establish a Statewide Fraud Awareness Campaign

We recommend that the State of Alabama establish and maintain a coordinated statewide fraud awareness campaign that provides residents with consistent, accurate, and timely information regarding cyber-enabled financial crimes. Our team suggests that Alabama should develop a recognizable campaign brand and hashtag, such as #StopFraudAL, to serve as the unified identity for fraud prevention messaging across participating state agencies. Similar statewide initiatives include Tennessee's CyberSafeTN (State of Tennessee, n.d.-b), Florida's Secure Florida (Florida Department of Law Enforcement, n.d.), and Kentucky's Stop Scams KY (Team Kentucky, n.d.). Drawing from these approaches, the campaign should utilize a dedicated public website, social media platforms, public service announcements, printable educational materials, and community outreach events to educate citizens about emerging fraud trends, cryptocurrency scams, identity theft, phishing schemes, and available reporting resources. A centralized campaign would create a trusted source of fraud prevention information, improve public recognition of scam warning signs, and promote consistent messaging across the state.

Our team recommends that Alabama should establish an ongoing collaborative partnership among ASC, the Alabama Law Enforcement Agency (ALEA), Banking, Office of the Attorney General, Alabama Department of Economic and Community Affairs (ADECA), local law

enforcement agencies, financial institutions, and other appropriate state partners to ensure the campaign remains coordinated and responsive to emerging threats. Participating agencies could join together to develop educational materials, share fraud trends and intelligence, and deliver unified public messaging through their respective communication channels, consistent with collaborative approaches implemented in California, Florida, and Kentucky (California Governor's Office of Emergency Services, n.d.; Florida Department of Law Enforcement, n.d.; Kentucky Office of Homeland Security, n.d.-b). Financial institutions could reinforce the campaign by distributing educational materials at branch locations, incorporating fraud prevention messaging into customer communications, and directing consumers to official state resources. Campaign effectiveness would be evaluated through measurable performance indicators, including website traffic, social media engagement, community outreach participation, and trends in consumer fraud reporting to ensure continuous improvement and responsible use of state resources.

Our team recommends that the State should provide recurring funding to support campaign administration and long-term sustainability. Initial funding would support campaign branding, development and maintenance of a centralized website, production of digital and printed educational materials, development of public service announcements, targeted social media advertising, and statewide outreach activities. Ongoing funding would sustain website maintenance, content updates, campaign evaluation, and continued public awareness efforts. Because participating agencies already maintain public information offices, websites, and communication platforms, many campaign activities can be integrated into existing state resources. Alabama could prioritize campaign planning and resource development during the first year, followed by phased implementation and continuous evaluation to ensure messaging remains current as fraud trends evolve.

Although implementation would require a modest annual investment, preventing even a small number of high-dollar fraud incidents can offset campaign costs. Individual victims of investment and cryptocurrency fraud frequently lose tens or hundreds of thousands of dollars, demonstrating that proactive consumer education has the potential to produce significant financial savings for Alabama residents while reducing investigative and enforcement burdens on state agencies. Collectively, this recommendation would shift Alabama's approach from reacting to fraud after

residents become victims to proactively preventing fraud through education, awareness, and coordinated partnerships. By institutionalizing a statewide awareness campaign supported by interagency collaboration, consistent branding, measurable performance metrics, and sustainable funding, Alabama could strengthen public awareness, encourage earlier reporting of fraud, and reduce financial losses resulting from cyber-enabled financial fraud, particularly investment and cryptocurrency-related scams.

Our team recommends establishing and maintaining a coordinated statewide fraud awareness campaign that leverages interagency collaboration, consistent public messaging, community partnerships, and digital outreach to educate residents about emerging cyber-enabled financial crimes. Supported by sustainable funding and measurable performance metrics, this campaign would strengthen fraud prevention efforts, encourage earlier reporting, and reduce financial losses associated with investment and cryptocurrency-related scams.

*The collaborative framework envisioned by this recommendation is illustrated in **Appendix B, Building Alabama's Fraud Prevention Network.***

Develop a Centralized Statewide Fraud Reporting and Resource Portal

We recommend that the State of Alabama should develop and maintain a centralized statewide fraud reporting and resource portal that serves as the official hub for fraud prevention information, victim assistance, and cyber-enabled financial crime reporting. Alabama currently provides multiple avenues for citizens to report suspected fraud and cyber incidents, including ASC's complaint process, OIT's cyber incident reporting resources, local law enforcement agencies, and federal reporting systems such as the FBI's Internet Crime Complaint Center (IC3) and CISA (ASC, 2026a; OIT, 2026; CISA, 2026; FBI, n.d.-c). While these reporting mechanisms provide valuable services within their respective jurisdictions, they operate independently and require citizens to navigate multiple websites and reporting processes. Similar statewide resources include Tennessee's Cyber Hub (State of Tennessee, n.d.-b), California's Cal-CSIC (California Governor's Office of Emergency Services, 2026), Florida's Secure Florida (Florida Department of Law Enforcement, n.d.), and Kentucky's Stop Scams KY (Team Kentucky, n.d.). Drawing from these approaches, we recommend that Alabama establish a single, state-managed

online portal that consolidates educational resources, reporting guidance, scam alerts, victim assistance, and access to existing reporting systems. The statewide fraud awareness campaign described in Recommendation One would identify this portal as Alabama's official source for fraud prevention information, reporting guidance, and victim assistance.

Rather than replacing existing reporting systems, the portal could integrate and coordinate Alabama's current reporting infrastructure. ASC, ALEA, Banking, Office of the Attorney General, OIT, ADECA, local law enforcement agencies, and other appropriate partners will collaborate to maintain the portal and adopt standardized reporting procedures. The portal would guide citizens to the appropriate reporting mechanism based on the nature of the complaint while allowing participating agencies to share standardized, nonconfidential reporting data for statewide analysis. This coordinated approach could simplify the reporting process, improve interagency communication, reduce public confusion regarding where complaints should be submitted, and strengthen collaboration without duplicating existing agency responsibilities.

To improve statewide intelligence gathering and trend analysis, participating agencies could adopt standardized reporting fields whenever practical. At a minimum, collected information would include the county or municipality where the fraud occurred; the fraud scheme involved (such as investment fraud, romance scams, pig butchering, business email compromise, phishing, or identity theft); the suspected method of initial contact (including email, text message, telephone call, social media, dating applications, or messaging platforms); the payment method or currency used (including cryptocurrency, wire transfers, gift cards, electronic payment applications, checks, or cash); digital asset wallet addresses, when applicable; estimated financial losses; victim demographics, when appropriate; and whether the incident was reported to local law enforcement. Standardized reporting would enable participating agencies to identify geographic fraud patterns, emerging scam trends, and areas requiring targeted education and enforcement while supporting evidence-based policy decisions.

In addition to serving as a reporting resource, the portal would feature a public-facing dashboard displaying aggregated statewide fraud statistics while protecting personally identifiable information. Rather than replacing agency-specific reporting, the dashboard would combine

nonconfidential information voluntarily shared by participating agencies to provide a broader picture of cyber-enabled financial crime across Alabama. Dashboard metrics might include reported financial losses, common fraud schemes, methods of initial contact, payment methods used by offenders, geographic distribution of reported incidents, and reporting trends over time. Quarterly summaries highlighting emerging fraud trends, significant scam patterns, and educational priorities could support coordinated outreach efforts and provide timely warnings to the public.

We recommend implementation to take place in a phased approach, beginning with development of the centralized website, standardized reporting guidance, and interagency coordination procedures, followed by integration of participating agencies and expansion of public-facing data reporting. Because many Alabama agencies already maintain fraud education materials, complaint forms, and cybersecurity resources, the portal would consolidate these existing resources into a single, user-friendly platform rather than duplicating agency services. This approach would improve accessibility for citizens while maximizing the value of existing state investments.

Although implementation will require funding for website development, cybersecurity protections, database integration, and ongoing maintenance, leveraging Alabama's existing reporting systems and educational resources could reduce duplication and improve efficiency. More importantly, a centralized portal would strengthen coordination among participating agencies, improve statewide fraud trend analysis, enhance public transparency, and support evidence-based decisions regarding fraud prevention, consumer education, and law enforcement resource allocation.

Our team recommends that the State of Alabama should develop and maintain a centralized statewide fraud reporting and resource portal that builds upon, rather than replaces, the reporting systems already maintained by state and federal agencies. By consolidating fraud prevention resources, providing clear reporting guidance, integrating existing complaint mechanisms, standardizing data collection where practical, and publishing aggregated statewide fraud trends through a public dashboard, Alabama would improve interagency coordination,

strengthen public awareness, enhance statewide data analysis, and better protect residents from cyber-enabled financial crime, including investment and cryptocurrency-related fraud.

*A conceptual illustration of how Alabama residents could access coordinated reporting and support resources is provided in **Appendix C, Finding Help When It Matters Most**.*

Establish a Lifelong Fraud Prevention Education Program

We recommend that the State of Alabama should establish a lifelong fraud prevention education program that provides residents with age-appropriate financial literacy and fraud awareness throughout every stage of life. Building upon educational models implemented in Kentucky through digital citizenship education (Kentucky Department of Education, 2025), Tennessee through student cybersecurity education and workforce-development resources (State of Tennessee, n.d.-a), Florida through statewide cybersecurity awareness and education (Florida Department of Law Enforcement, n.d.), and New York through targeted fraud-prevention education for older adults (New York Department of State, 2023), Alabama could integrate fraud prevention education into K–12 schools, community colleges, financial institutions, retirement planning programs, and community-based senior services to improve residents' ability to recognize, avoid, and report cyber-enabled financial crimes. National youth cybersecurity programs such as CyberPatriot and GenCyber also provide educational models for introducing students to cybersecurity concepts and hands-on learning (CyberPatriot, n.d.; Department of Defense Cyber Exchange, n.d.). California's state-funded Cyber-Seniors programs further demonstrate an approach to supporting technology and digital literacy education for older adults (California Public Utilities Commission, 2026). The team believes that providing consistent education throughout multiple stages of life would strengthen Alabama's long-term fraud prevention efforts while reinforcing the statewide awareness campaign and centralized reporting and resource portal described in Recommendations One and Two.

The team believes that the Alabama State Department of Education should incorporate a standardized financial literacy and fraud prevention module into existing high school coursework, such as Health or Career Preparedness. Alabama's community colleges would incorporate fraud prevention education into existing financial literacy, workforce development, or continuing

education programs to reach adult learners entering or reentering the workforce. Educational content could include budgeting, responsible financial decision-making, digital financial safety, identity protection, investment fundamentals, cryptocurrency basics, recognizing common fraud schemes, identifying scam red flags, and understanding how and where to report suspected fraud. Instruction should emphasize real-world scenarios involving investment fraud, romance scams, phishing attacks, impersonation scams, cryptocurrency fraud, and other emerging cyber-enabled financial crimes to prepare students before they enter adulthood.

We recommend that Banking should partner with state-chartered financial institutions to strengthen fraud prevention education for both employees and consumers. Bank employees would receive standardized training to recognize indicators of financial exploitation, identify suspicious transactions, respond appropriately to suspected fraud, and understand available reporting procedures. In addition, state-chartered financial institutions should provide new account holders with a brief fraud awareness education requirement through a short video, digital module, or informational pamphlet explaining common scam tactics, warning signs, methods for reporting suspected fraud, and resources available through the financial institution, local law enforcement, and the State of Alabama. Standardizing customer education when an account is opened would help ensure that consumers receive fraud prevention information before becoming victims rather than after financial losses have occurred.

Our team believes that ASC, in collaboration with the Retirement Systems of Alabama (RSA), state retirement administrators, financial institutions, and other appropriate partners, should develop standardized fraud prevention education for individuals making an initial withdrawal from retirement accounts, including pensions, 401(k) plans, individual retirement accounts, and other retirement savings vehicles. Prior to completing an initial withdrawal, individuals should receive a brief educational video, digital module, or printed material explaining common investment scams, cryptocurrency fraud, impersonation schemes, and other fraud tactics that frequently target retirement assets. Educational materials would also explain available reporting resources and encourage individuals to verify unexpected financial requests before transferring retirement funds.

It is our team's recommendation that the Alabama Department of Senior Services could collaborate with local senior centers, Area Agencies on Aging, public libraries, community colleges, and other community organizations to provide recurring fraud prevention and financial literacy education for older adults. Senior centers could offer monthly or bimonthly educational sessions addressing current fraud trends, emerging scam tactics, safe online practices, investment fraud, cryptocurrency scams, and available victim resources. Similar to California's support of Cyber-Seniors programs and New York's senior-focused outreach initiatives, these community-based educational opportunities would provide older adults with ongoing access to trusted information as fraud schemes continue to evolve (California Public Utilities Commission, 2026; New York Department of State, 2023).

*The implementation pathway outlined in this recommendation is summarized visually in **Appendix D, From Vision to Action**.*

Our team recommends that implementation should occur through a phased approach, beginning with development of standardized educational materials and training modules during the first year, followed by integration into school curricula, community college programming, then state-chartered financial institutions, retirement education programs, and finally senior center programming. Existing educational materials and training resources developed by participating agencies would be incorporated whenever practical to reduce implementation costs while maintaining consistent statewide messaging. Educational materials should be reviewed and updated annually to reflect an evaluation of emerging fraud trends, technological advances, and evolving scam tactics. Program effectiveness could be evaluated through participation rates, pre- and post-training knowledge assessments, educator and participant feedback, and trends in reported fraud involving students, banking customers, and older adults. We suggest that educational materials should consistently direct residents to Alabama's statewide fraud awareness campaign and centralized fraud reporting portal to reinforce public education and encourage timely reporting.

Although implementation would require investments in curriculum development, educational materials, staff training, and program coordination, the team believes that many components

could be integrated into existing educational programs and outreach initiatives, reducing long-term costs. Preventing a relatively small number of investment and cryptocurrency fraud incidents among students, banking customers, and retirees has the potential to offset implementation costs through reduced financial losses and decreased demand for investigative and victim assistance resources. Collectively, these educational initiatives would establish a lifelong fraud prevention framework that equips Alabama residents with the knowledge necessary to recognize, prevent, and report financial fraud at every stage of life. By institutionalizing fraud prevention education through trusted community partners, Alabama could shift from responding to fraud after it occurs to proactively preparing residents to identify and avoid scams before financial losses occur.

Our team suggests that the State of Alabama should establish a lifelong fraud prevention education program by integrating financial literacy and scam awareness into K–12 schools, community colleges, state-chartered financial institutions, retirement education and planning, and senior services programming. Delivered through trusted educational, financial, and community partners, and reinforced by Alabama’s statewide awareness campaign and centralized fraud reporting portal, the program would improve financial literacy, encourage earlier fraud reporting, reduce victimization, and better protect residents from investment and cryptocurrency-related scams. A lifelong approach would recognize that fraud risks evolve throughout an individual’s life and that effective prevention requires education at key financial decision points, from adolescence through retirement.

*The lifelong approach to fraud prevention education envisioned by this recommendation is illustrated in **Appendix E, Protecting Alabamians Across Every Stage of Life.***

CONCLUSION

Cyber-enabled financial crime will continue to evolve in both sophistication and frequency, making proactive prevention, public education, and coordinated action increasingly important. Alabama has already established a strong foundation through its existing agencies, partnerships, and recent legislative initiatives. Building upon Alabama's existing foundation will strengthen the State's ability to prevent, detect, and respond to emerging cyber-enabled financial fraud.

By implementing these recommendations, Alabama can create a more coordinated, informed, and resilient approach to protecting Alabama residents from investment fraud, cryptocurrency scams, and other cyber-enabled financial crimes. The goal is not merely to respond to cyber-enabled fraud, but to help create a digitally and financially literate Alabama that is prepared to recognize, resist, and report fraud. Through sustained collaboration among government agencies, educational institutions, financial organizations, community partners, and the public, Alabama can reduce financial losses, safeguard and strengthen public trust, and position itself as a national leader in proactive fraud prevention and consumer protection.



PROTECT
Stay informed.



PREVENT
Spot the signs.



PARTNER
Stronger together.

#StopFraudAL

REFERENCES

Alabama Department of Economic and Community Affairs. (2024a). *Alabama Digital Opportunity Plan*. <https://adeca.alabama.gov/wp-content/uploads/Alabama-Statewide-Digital-Opportunity-Plan.pdf>

Alabama Department of Economic and Community Affairs. (2024b). *Broadband Equity, Access, and Deployment (BEAD) Five-Year Action Plan Summary*. <https://adeca.alabama.gov/wp-content/uploads/Alabama-BEAD-Five-Year-Action-Plan-Summary.pdf>

Alabama Office of Information Technology. (2026). *For citizens*. <https://oit.alabama.gov/for-citizens/>

Alabama Securities Commission. (2023a). *The fraud file*. <https://asc.alabama.gov/wp-content/uploads/2023/11/fraud-file.pdf>

Alabama Securities Commission. (2023b). *Guidelines for protecting vulnerable adults from financial exploitation*. <https://asc.alabama.gov/wp-content/uploads/2023/11/Guidelines-ALA-CODE-8-6-170-et-seq.pdf>

Alabama Securities Commission. (2024). *Scam alerts*. <https://asc.alabama.gov/for-investors/investor-education/scam-alert/>

Alabama Securities Commission. (2025). *FY 2024 annual report*. <https://asc.alabama.gov/wp-content/uploads/2025/11/FY-2024-Annual-Report.pdf>

Alabama Securities Commission. (2026a). *Procedure for filing a complaint with the Alabama Securities Commission*. <https://asc.alabama.gov/for-industry/enforcement/complaint-procedure/>

Alabama Securities Commission. (2026b). *She Can*. <https://asc.alabama.gov/for-investors/she-can/>

Alabama Securities Commission. (2026c, April 9). *Stablecoin legislation signed by Governor Ivey*. <https://asc.alabama.gov/wp-content/uploads/2026/04/Stablecoin-Legislation.pdf>

Alabama Securities Commission. (n.d.). *Mission*.

<https://asc.alabama.gov/about/mission/>

Alabama State Banking Department. (2026). *Fiscal year 2025 annual report*.

<https://banking.alabama.gov/wp-content/uploads/2026/02/FY-2025-Annual-Report.pdf>

Bowerman, A. (2022, November 11). *Montgomery County DA warns of sextortion scams targeting teen boys*. WSFA 12 News.

<https://www.wsfa.com/2022/11/12/montgomery-county-da-warns-sextortion-scams-targeting-teen-boys/>

California Governor's Office of Emergency Services. (2026, May 28). *Cal-CSIC services & capabilities: Cybersecurity support for California partners*. <https://www.caloes.ca.gov/wp-content/uploads/Homeland-Security/Documents/Services/Cal-CSIC-Services-Quick-Reference.pdf>

California Governor's Office of Emergency Services. (n.d.). *Cal-CSIC mission*.

<https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/cal-csic-mission/>

California Public Utilities Commission. (2026, February 26). *CPUC awards millions to expand digital literacy and broadband access across California*.

<https://www.cpuc.ca.gov/news-and-updates/all-news/cpuc-awards-millions-to-expand-digital-literacy-and-broadband-access-across-california>

Consensys. (2026). *Clipboard hacking*. <https://support.metamask.io/stay-safe/protect-yourself/wallet-and-hardware/clipboard-hacking/>

Cryptocurrency Kiosk Fraud Prevention Act, H.B. 303, 2026 Reg. Sess. (Ala. 2026).

<https://alison.legislature.state.al.us/files/pdf/SearchableInstruments/2026RS/HB303-enr.pdf>

CyberPatriot. (n.d.). *What is CyberPatriot?*

<https://www.uscyberpatriot.org/Pages/About/What-is-CyberPatriot.aspx>

Cyber-Seniors. (n.d.). *Cybersecurity center*. <https://cyberseniors.org/cybersecurity/>

Cybersecurity and Infrastructure Security Agency. (n.d.-a). *Glossary*. National Initiative for Cybersecurity Careers and Studies. <https://niccs.cisa.gov/about-niccs/glossary>

Cybersecurity and Infrastructure Security Agency. (n.d.-b). *Require multifactor authentication*. <https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/require-multifactor-authentication>

Cybersecurity and Infrastructure Security Agency. (2024). *Phishing*. https://www.cisa.gov/sites/default/files/2024-02/Update%20to%20Phishing%20General%20Security%20Postcard_01.01.2024.pdf

Cybersecurity and Infrastructure Security Agency. (2026). *Incident reporting form*. <https://myservices.cisa.gov/irf>

Department of Defense Cyber Exchange. (n.d.). *GenCyber*. <https://www.cyber.mil/gencyber/>

Federal Bureau of Investigation. (2024). *2024 cryptocurrency state report: Alabama*. Internet Crime Complaint Center. <https://www.ic3.gov/AnnualReport/Reports/2024CryptocurrencyState/>

Federal Bureau of Investigation. (2026). *Internet crime report 2025*. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

Federal Bureau of Investigation. (n.d.-a). *Business email compromise*. <https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise>

Federal Bureau of Investigation. (n.d.-b). *Cryptocurrency investment fraud*. <https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud>

Federal Bureau of Investigation. (n.d.-c). *Directing your complaint*. Internet Crime Complaint Center. <https://www.ic3.gov/Home/DirectComplaint>

Federal Trade Commission. (2022, May). *What to know about cryptocurrency and scams.*

Consumer Advice. <https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-scams>

Federal Trade Commission. (2023, July). *How to avoid a scam.* Consumer Advice.

<https://consumer.ftc.gov/articles/how-avoid-scam>

Federal Trade Commission. (2025a). *Consumer Sentinel Network data book 2024.*

<https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024>

Federal Trade Commission. (2025b, March). *New FTC data show big jump in reported losses to fraud to \$12.5 billion in 2024.* [https://www.ftc.gov/news-events/news/press-](https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024)

[releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024](https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024)

Financial Innovation and Market Expansion Act, H.B. 259, 2026 Reg. Sess. (Ala. 2026).

<https://alison.legislature.state.al.us/files/pdf/SearchableInstruments/2026RS/HB259-enr.pdf>

Florida Center for Cybersecurity. (n.d.-a). *Mission & history.* University of South Florida.

<https://cyberflorida.org/about/>

Florida Center for Cybersecurity. (n.d.-b). *Safer connecting.* University of South Florida.

<https://cyberflorida.org/safer-connecting/>

Florida Department of Law Enforcement. (n.d.). *About us.* Secure Florida.

<https://www.secureflorida.org/AboutUs.htm>

Fox10TV. (2024, September 20). *Mobile police warn of threatening email, scammers attempting to extort victims for cryptocurrency.* [https://fox10tv.com/2024/09/20/mobile-police-warn-](https://fox10tv.com/2024/09/20/mobile-police-warn-threatening-email-scammers-attempting-extort-victims-cryptocurrency/)

[threatening-email-scammers-attempting-extort-victims-cryptocurrency/](https://fox10tv.com/2024/09/20/mobile-police-warn-threatening-email-scammers-attempting-extort-victims-cryptocurrency/)

Henry, B. (2026, January 27). *Alabama lawmaker proposes bill to protect consumers from crypto ATM scams.* WSFA 12 News. [https://www.wsfa.com/2026/01/27/alabama-lawmaker-proposes-](https://www.wsfa.com/2026/01/27/alabama-lawmaker-proposes-bill-protect-consumers-crypto-atm-scams/)

[bill-protect-consumers-crypto-atm-scams/](https://www.wsfa.com/2026/01/27/alabama-lawmaker-proposes-bill-protect-consumers-crypto-atm-scams/)

Kentucky Department of Education. (2025, January 30). *Digital citizenship.*

<https://www.education.ky.gov/school/diglrn/digcitizen>

Kentucky Office of Homeland Security. (n.d.-a). *Cybersecurity*.

<https://homelandsecurity.ky.gov/Pages/Cybersecurity.aspx>

Kentucky Office of Homeland Security. (n.d.-b). *Mission statement*.

<https://homelandsecurity.ky.gov/About/Pages/Mission-Statement.aspx>

National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*.

<https://doi.org/10.6028/NIST.AI.100-1>

National Institute of Standards and Technology. (2024). *Artificial intelligence risk management framework: Generative artificial intelligence profile (NIST AI 600-1)*.

<https://doi.org/10.6028/NIST.AI.600-1>

National Institute of Standards and Technology. (n.d.). *Glossary*. Small Business Cybersecurity Corner. <https://www.nist.gov/itl/smallbusinesscyber/training/glossary>

National Security Agency Office of the Inspector General. (2022, March 10). *Slam the Scam Day: Protect yourself from government imposter scams*.

<https://oig.nsa.gov/Media/Article/2962364/slam-the-scam-day-protect-yourself-from-government-imposter-scams/>

New York Department of State. (2023, June). *S.A.F.E.: Senior anti-fraud education*. Division of Consumer Protection.

<https://dos.ny.gov/senior-anti-fraud-education-safe>

New York Department of State. (2025, December 1). *Consumer alert: Ahead of Cyber Monday, the NYS Department of State's Division of Consumer Protection warns shoppers about AI-generated fraud and scams online*.

<https://dos.ny.gov/node/83401>

New York Department of State. (n.d.-a). *Consumer outreach presentations*. Division of Consumer Protection.

<https://dos.ny.gov/consumer-outreach-presentations-0>

New York Department of State. (n.d.-b). *File a complaint online*. Division of Consumer Protection.

<https://cpp.dos.ny.gov/>

New York State Department of Financial Services. (n.d.). *Scams, fraud, and cyber crime*.

https://www.dfs.ny.gov/consumers/fraud_cyber_protection

New York State Office of the Attorney General. (2024, July 9). *Attorney General James urges New Yorkers to use free credit monitoring and identity theft protection services in aftermath of Change Healthcare cyberattack*.

<https://ag.ny.gov/press-release/2024/attorney-general-james-urges-new-yorkers-use-free-credit-monitoring-and-identity>

New York State Office of the Attorney General. (n.d.). *File a complaint*.

<https://ag.ny.gov/file-complaint>

SARCOA. (2026). *Fraud Summit*. <https://sarcoa.org/event/fraud-summit-2/>

Schuessler, S. (2025, November 20). *Crypto ATM scams rising, stealing millions from Alabamians; how to be vigilant*. WSFA 12 News.

<https://www.wsfa.com/2025/11/21/crypto-atm-scams-rising-stealing-millions-alabamians-how-be-vigilant/>

State of Tennessee. (n.d.-a). *Higher Ed cyber resources in TN*. Tennessee Cyber Hub.

<https://www.tn.gov/cybersecurity/tn-citizens-cybersecurity/tn-citizens-cybersecurity---for-students/post-secondary-options-for-students/tn-cyber-student-resources.html>

State of Tennessee. (n.d.-b). *Tennessee Cyber Hub*.

<https://www.tn.gov/cybersecurity.html>

Team CommUNITY. (n.d.). *What is digital literacy? And why it matters*. Digital Rights Community.

<https://www.digitalrights.community/blog/what-is-digital-literacy>

Team Kentucky. (n.d.). *Stop Scams*. <https://stopscams.ky.gov/>

The Homewood Star. (2026, March 19). *Cybersecurity basics*.

https://thehomewoodstar.com/events/cybersecurity-basics/?occ_dtstart=2026-04-09T15%3A00

United States Postal Inspection Service. (2025, February 20). *Quishing*.

<https://www.uspis.gov/news/scam-article/quishing>

University of South Alabama. (2025). *CyberSmart*.

<https://www.southalabama.edu/departments/csc/informationsecurity/cybersmart/>

LEARNING FROM LEADING STATES

Applying Proven Practices to Strengthen Alabama's Response to Cybercrime & AI-Fraud

Across the nation, states are innovating, collaborating, and achieving results.
Alabama learns. Alabama leads.



We look outward to move forward.

Alabama learns from what works—then adapts it to serve our state.



WE LEARN TOGETHER

from leading states who are advancing cybercrime prevention through innovation, data, and partnership.



WE BRING IT HOME

adapting what works best to strengthen Alabama's response and build public trust.

FIVE STATES. ONE LESSON.



CALIFORNIA

Strong consumer education and outreach.

Clear messaging and accessible resources empower consumers.



FLORIDA

Coordinated reporting pathways and public tools.

Simple, effective reporting systems make it easier to take action.



KENTUCKY

Advanced data analytics and risk detection.

Data-driven tools help identify threats earlier and more accurately.



TENNESSEE

Strong partnerships across agencies and industries.

Collaboration multiplies impact and extends resources.



NEW YORK

Public education that builds awareness and resilience.

Awareness today strengthens communities for tomorrow.



Strong Partnerships Across Agencies and Industries
Collaboration multiplies impact.



THREE PRACTICES EMERGE

Data-Informed Prevention and Early Intervention
Information today prevents harm tomorrow.



Public Education That Empowers Consumers
Awareness today strengthens resilience.

Alabama learns. Alabama adapts. Alabama protects.

Together, we build a safer, stronger Alabama.

APPENDIX B

BUILDING ALABAMA'S FRAUD PREVENTION NETWORK

Coordinated Partners for Public Protection

*No one agency can do this alone.
Together, we create stronger protection for every Alabamian.*



OUR SHARED PRINCIPLES



SHARED RESPONSIBILITY

Everyone has a role in protecting the public.



TRUST & COLLABORATION

Strong relationships create stronger outcomes.



EARLY DETECTION & PREVENTION

Timely information helps stop fraud before it spreads.



ACCOUNTABILITY & INTEGRITY

We uphold the highest standards in every action.



PROTECTING ALABAMA

Our coordination today builds a safer, stronger Alabama tomorrow.



PROTECTING ALABAMA REQUIRES EVERY PARTNER DOING WHAT IT DOES BEST, TOGETHER.

One network. One mission. One Alabama.

FINDING HELP WHEN IT MATTERS MOST

One Trusted Path. Many Resources. Real Support.

Alabama's Central Access Point connects people to trusted help quickly, confidentially, and effectively.



★ HOW IT WORKS ★

1 REACH OUT

Individuals, families, or professionals contact the Central Access Point.



2 GET GUIDED

Trained specialists listen, assess needs, and provide clear next steps.



3 GET CONNECTED

You're connected to the right resources and services in your community.



4 GET SUPPORT

Ongoing support and follow-up ensure no one faces the journey alone.



OUR COMMITMENT



COLLABORATION

Stronger together across agencies and communities.



COMPASSION

Every person deserves dignity, respect, and care.



ACCOUNTABILITY

We measure progress and strive for excellence.



EQUITY

Ensuring every Alabamian can access help.

FROM VISION TO ACTION

A Roadmap for Results. A Commitment to Alabama.

Turning shared goals into measurable progress to reduce fraud and protect our communities.



A SAFER ALABAMA

Through collaboration, innovation, and determination.

VISION
PLAN
PARTNERSHIP

ACTION
IMPACT

OUR GUIDING PRINCIPLES



COLLABORATION
Stronger together across agencies and communities.



PREVENTION
Stopping fraud before it starts.



ACCOUNTABILITY
Using data and oversight to drive continuous improvement.



ACCESS
Ensuring every Alabamian can get the help they need.



INTEGRITY
Upholding trust, transparency, and ethical leadership.

OUR ROADMAP TO A FRAUD-RESILIENT ALABAMA

1

ALIGN OUR EFFORTS

Strengthen coordination across agencies and partners.



2

BUILD CAPACITY

Invest in tools, training, and technology that empower our network.



3

EDUCATE & ENGAGE

Raise awareness and equip Alabamians with knowledge and resources.



4

DETECT & RESPOND

Enhance data sharing and investigative capabilities.



5

MEASURE & IMPROVE

Track results, learn, and continuously strengthen our impact.



TODAY'S ACTIONS. TOMORROW'S SAFER ALABAMA.

Our commitment is clear. Our path is set.
Together, we will deliver lasting results and protect what matters most—our people.



OUR COMMITMENT



PROTECT THE PUBLIC

Safeguard Alabamians from financial harm and exploitation.



STRENGTHEN PARTNERSHIPS

Unite government, private sector, and communities.



DRIVE INNOVATION

Use data and technology to stay ahead of emerging threats.



UPHOLD INTEGRITY

Act with transparency, fairness, and accountability.



DELIVER RESULTS

Measure what matters and make a difference every day.

APPENDIX E

PROTECTING ALABAMIANS Across Every Stage of Life

Trusted Resources. Stronger Communities. A Safer Alabama.

From childhood to older adulthood,
Alabama's fraud prevention and support
network is here to **help, protect, and empower.**

PROTECTION ACROSS THE LIFESPAN



PREVENT FRAUD
Stopping harm before
it happens through
education and vigilance.



PROVIDE SUPPORT
Connecting individuals
to trusted help and
essential resources.



PROMOTE RECOVERY
Supporting healing,
restoration, and a
path forward.



**STRENGTHEN
COMMUNITIES**
Working together for
safe, resilient, and
thriving communities.



**PROTECT OUR
FUTURE**
Ensuring every generation
has the support and
opportunity to thrive.



ONE STATE. ONE PURPOSE.

Protecting People. Building Trust. Strengthening Alabama.

SUPPORT AT EVERY STAGE



OUR COMMITMENT TO EVERY ALABAMIAN



LISTEN

We hear your needs
and learn from your
experiences.



ACT

We take action with
urgency, transparency,
and care.



COLLABORATE

We work together across
agencies, communities,
and generations.



PROTECT

We safeguard individuals
from fraud, harm,
and exploitation.



EMPOWER

We provide tools,
knowledge, and hope
for a stronger tomorrow.

When we protect each person, we strengthen every community—today and for generations to come.