Entrepreneurial Opportunities in Cybersecurity: Scam Detection and AI Media Verification

Liana Davis

Old Dominion University

CPD/CYSE 494

Professor Rob Batchelder

February 16, 2026

Venture Idea 1: Scam Smart - Multi-Platform Verification

Scam Smart is a mobile application designed to help users verify whether digital messages are legitimate or fraudulent. The app allows individuals to paste text, upload screenshots, or forward suspicious emails, direct messages, or text messages for analysis. Using pattern recognition and scam-detection algorithms, the system evaluates language cues, impersonation tactics, urgency indicators, and suspicious links. It then provides a clear risk rating along with a simple explanation and recommended next steps. This venture focuses on empowering everyday users to make informed decisions before responding to potentially harmful communications.

The Growing Threat of Digital Scams

Digital scams are becoming more advanced and frequent across multiple communication platforms. Phishing attempts no longer occur only through email; they now appear in text messages, social media direct messages, job recruitment platforms, and even professional networking sites. Many of these scams create a sense of urgency or fear, pressuring individuals to act quickly before thinking critically. As artificial intelligence improves, scam messages are becoming more convincing and harder to detect. While email providers and phone carriers attempt to filter spam, these systems are inconsistent and do not provide users with clear explanations. As a result, individuals often feel uncertain and must rely on guesswork or informal advice from friends when deciding whether a message is safe.

Market Potential and Revenue Model

The demand for Scam Smart is strong because nearly every smartphone user is exposed to digital scams. As communication increasingly shifts to online platforms, the number of opportunities for fraud continues to grow. This creates a broad target market that includes college students, working professionals, older adults, and small business owners. Because the application is fully digital, it is highly scalable and can expand nationally or globally without significant physical overhead costs. The venture could operate using a freemium model, offering limited free scans while charging a monthly subscription for unlimited message verification and advanced analysis features. This recurring revenue structure provides long-term profitability while keeping the service accessible to users.

Risks and Challenges

Although Scam Smart presents strong market potential, several challenges must be addressed. The accuracy of the detection system is critical, as false positives could cause users to distrust legitimate messages, while false negatives could expose users to harm. Data privacy is another major concern, since users would be uploading personal communications for analysis. The company would need to implement strict encryption and transparent data policies to build trust. Additionally, competition from built-in spam filters and existing security tools could limit market share. To remain competitive, the venture would need to differentiate itself through clarity, ease of use, and reliable explanations rather than purely technical detection.

Discovery Process / Design Thinking

The idea for Scam Smart emerged from observing how frequently individuals question the legitimacy of digital messages. Many people take screenshots of suspicious texts or emails and send them to friends or family members asking for reassurance before responding. This behavior highlights a clear gap in the market: users want quick verification from a trusted source. Applying principles of design thinking, this venture centers on understanding user anxiety, confusion, and time pressure when faced with potential scams. Instead of focusing solely on technical detection, the concept prioritizes simplicity, clarity, and emotional reassurance. By designing the platform around real user behavior and decision-making patterns, Scam Smart aims to provide both protection and confidence in digital communication.

Venture Idea 2: AI Authenticity - Fake Media and News Detection

AI Authenticity is a digital application designed to help users determine whether online media is genuine or artificially generated. The platform allows individuals to upload photos, videos, or links to news articles for analysis. Using AI detection tools and source verification systems, the application evaluates whether content has been manipulated, generated by artificial intelligence, or published by unreliable sources. It then provides users with a credibility rating along with a brief explanation of its findings. The goal of this venture is to help individuals navigate an increasingly complex digital environment where distinguishing between real and fabricated content is becoming more difficult.

The Challenge of Digital Authenticity

The rapid advancement of artificial intelligence has made it increasingly difficult for individuals to distinguish between genuine and manipulated content online. AI tools can now generate realistic images, videos, and written news articles that closely resemble authentic material. As a result, misinformation can spread quickly across social media platforms and digital news outlets. This creates serious risks, including reputational damage, political manipulation, financial fraud, and social engineering attacks. Unlike traditional scams that rely on suspicious links or obvious errors, AI-generated content often appears polished and believable. Without accessible verification tools, users are left to rely on personal judgment in a digital environment where deception is becoming harder to detect.

Market Potential and Revenue Model

The demand for digital authenticity tools is expanding as artificial intelligence reshapes how information is created and distributed. News organizations, educational institutions, businesses, and everyday social media users are increasingly concerned about the credibility of online content. Unlike scam detection, which focuses on individual messages, this venture addresses a broader trust crisis affecting public discourse and digital communication as a whole. Because misinformation can influence elections, financial markets, and public safety, organizations have strong incentives to adopt verification tools. Revenue could be generated through a tiered subscription model for individual users, as well as institutional licensing for schools, media outlets, and corporate communication teams. This dual market approach increases long-term growth potential beyond individual consumers.

Risks and Challenges

Despite its potential, this venture faces several significant challenges. The rapid advancement of generative AI means that detection systems must continuously evolve to keep pace with increasingly realistic synthetic media. If the platform fails to maintain high accuracy, users may lose trust in its credibility assessments. There is also the risk of overreliance, where users assume the tool is always correct without applying critical thinking. Additionally, large technology companies may develop similar verification features within their own platforms, increasing competition. To remain viable, the venture would need to prioritize accuracy, transparency in its detection process, and ongoing technological updates to adapt to emerging AI capabilities.

Comparative Analysis

Both ventures address growing challenges within the cybersecurity landscape, but they focus on different dimensions of digital risk. Scam Smart concentrates on protecting individuals from direct financial fraud through message-based scams, including texts, emails, and direct messages. It targets everyday users who face immediate and personal consequences from phishing and social engineering attacks. In contrast, AI Authenticity focuses on verifying digital media content by detecting manipulated images, AI-generated videos, and misleading news sources. While Scam Smart responds to individual security threats, AI Authenticity addresses broader risks involving misinformation, reputational harm, and digital deception. Both ideas are scalable and operate within the cybersecurity domain, but they differ in scope and target audience.

When evaluating long-term impact, AI Authenticity appears to address a more urgent and evolving individual need. While Scam Smart targets financial scams that many users may feel confident identifying on their own, AI-generated media presents a newer and less understood threat. Individuals often rely on their personal judgment when evaluating suspicious messages, but manipulated images, videos, and fabricated news stories can be far more difficult to detect without technical assistance. As artificial intelligence tools continue to improve, distinguishing between authentic and synthetic content will likely become increasingly challenging. For this reason, AI Authenticity may serve as a more necessary tool for individuals seeking clarity in a rapidly changing digital environment. Although both ventures demonstrate strong potential, AI Authenticity addresses a deeper issue of digital trust that may have longer-term societal implications.

References

Federal Bureau of Investigation. (2024). *Internet crime report 2023*. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf