1. Fraud-as-a-Service

Fraud-as-a-service (FaaS) involves criminals accessing machine learning, generative Artificial Intelligence (AI), predictive analytics, and other tools to help them commit fraud.

**MITIGATION STRATEGY:** Establish, adopt, and enforce agency-wide policies to promote awareness. Implement a device risk mitigation workflow.

2. Account Takeover Fueled by Synthetic Identities

Account takeover attacks have become a major threat, with criminals misappropriating or abusing identities to gain access to accounts. Synthetic identities—brand-new identities—create numerous issues for government agencies.

**MITIGATION STRATEGY:** Ensure identity composition and risk elements are front and center. Consider introducing biometrics to mitigate FaaS risk.

3. Artificially Intelligent Fraudsters

Fraudsters are accessing machine learning, generative AI, predictive analytics, and other advanced tools to commit fraud, making it difficult to detect synthetic identities.

**MITIGATION STRATEGY:** Ensure identity composition and risk elements are front and center as fraud-as-a-service takes off. Establish, adopt, and enforce agency-wide policies to promote awareness.

4. Serious Cyberthreats

Recent breaches have affected government agencies, demonstrating that protection is crucial. Criminals are using tools to manipulate systems and commit fraud.

**MITIGATION STRATEGY:** Ensure identity composition and risk elements are front and center. Establish, adopt, and enforce agency-wide policies to promote awareness.

5. Worses About Windows

Windows users are prone to ransomware attacks. Criminals are bypassing two-factor authentication (2FA) and using phishing emails to trick users into thinking they are legitimate.

**MITIGATION STRATEGY:** Ensure identity composition and risk elements are front and center. Establish, adopt, and enforce agency-wide policies to promote awareness.

6. A Cashsly Society

In a June 2023 survey of 650 cybersecurity experts, three out of four experts polled noted that 2024 could be the year that criminals begin to employ AI and machine learning to automate attacks.

**MITIGATION STRATEGY:** Ensure identity composition and risk elements are front and center. Establish, adopt, and enforce agency-wide policies to promote awareness.

7. Reference Elder Fraud

Elder fraud is on the rise, and criminals are using synthetic identities to exploit this vulnerability. Government agencies should be aware of this threat.

**MITIGATION STRATEGY:** End elder fraud before it happens.

8. Digital Eats or Risk

Legitimate users may be at risk of digital impersonation. Criminals are using various tactics to gain access to users' accounts, including social engineering and phishing.

**MITIGATION STRATEGY:** Ensure identity composition and risk elements are front and center.