GetReal

Deepfakes:

Your Identity Systems Verify Credentials — Not People

“Deepfakes exploit the boundary where traditional IAM controls end and human judgement begins.”

What IAM Leaders Need to Know Now

The identity infrastructure you've built to secure access and enable authentication has a fundamental gap: it verifies that credentials are valid, not that the person presenting them is who they claim to be. AI-generated voice and video are now being used to impersonate legitimate users during live digital interactions, and at these moments identity is assumed based on appearance, voice, or video presence rather than cryptographic proof.

Deepfakes exploit the boundary where your technical controls end and human judgment begins. Multi-factor authentication confirms possession of a device. Single sign-on validates credentials. Biometric systems verify stored templates. But none of these prevent an attacker from using a deepfake to convince a help desk agent, HR representative, or executive to grant access, reset credentials, or modify security settings.

This creates a strategic vulnerability. Your IAM program secures the access layer, but identity verification during live interactions — onboarding, support calls, approval workflows — operates outside your systems. When those interactions fail, the consequence is still an identity and access failure. And as the IAM leader, you own the risk of unauthorized access regardless of where the control gap originated.

Why This Is an IAM Leadership Issue

Identity governance and access control have a new challenge: deepfakes that bypass authentication by exploiting the gap between technical verification and human judgment.

- **Identity strategy gap:** Your IAM architecture secures digital access, but doesn't address identity verification in human workflows (hiring, help desk, executive communications) where deepfakes enable impersonation
- **Control bypass through social engineering:** Attackers use deepfakes to manipulate people who have the authority to grant access, provision credentials, or override security controls rendering technical IAM protections irrelevant
- **Accountability for unauthorized access:** When deepfake-enabled impersonation results in unauthorized access, IAM leadership may be asked to explain why identity controls failed, even if the failure occurred in a workflow outside IAM's direct control
- **Cross-functional coordination challenges:** IAM sits at the intersection of Security, IT, HR, and business operations, and deepfake risks require IAM leaders to extend identity verification standards into processes owned by other functions
- **Experience vs. security tension:** IAM balances user experience with security, but deepfakes force a recalibration: verification methods that seem frictionless (voice and other biometrics) are no longer secure
- **Regulatory and audit exposure:** IAM programs are subject to audit and compliance requirements, and when identity verification fails due to deepfake impersonation, auditors and regulators will question whether IAM controls remained adequate given known threats

What "Reasonable Preparedness" Looks Like

Leading IAM programs are evolving beyond credential verification to address identity verification in live, human-mediated workflows:

- **Real-time deepfake detection:** Evaluate and pilot solutions that analyze voice and video for synthetic indicators during authentication and verification workflows
- **Liveness detection and biometric hardening:** Deploy anti-spoofing technologies that detect synthetic media in biometric authentication, preventing deepfake images and videos from bypassing facial recognition
- **Phishing-resistant authentication:** Transition to passkeys, FIDO2, and cryptographic authentication that cannot be replicated through deepfakes or social engineering
- **Out-of-band verification for high-risk actions:** Require identity verification through separate, pre-established channels for credential resets, MFA changes, privileged access requests, and account modifications
- **Identity verification in onboarding:** Extend IAM standards into HR hiring and onboarding processes, ensuring that identity is verified — not just visually confirmed via video interview

What “Reasonable Preparedness” Looks Like (*continued*)

- **Behavioral and contextual analytics:** Implement continuous authentication that analyzes behavior patterns, device characteristics, location, and interaction anomalies — factors that deepfakes cannot easily replicate
- **Enhanced logging and auditability:** Ensure comprehensive audit trails documenting “who verified whom, through which method, and what evidence was collected” for all identity-sensitive actions
- **Cross-functional identity governance:** Establish IAM oversight of identity verification across HR, IT support, customer service, and other functions where identity decisions create access risk

Real Consequences

Identity and access management systems are being bypassed through deepfake-enabled impersonation, with documented incidents showing that technical IAM controls cannot prevent these attacks:

- **Face-swapping deepfake attempts to bypass remote verification grew 700%** in 2023. (Source)
- **$25 million transferred at Arup** after an employee joined a video call with deepfaked executives. The attack succeeded because identity verification relied on visual/audio confirmation rather than cryptographic proof. (Source)
- **Account takeovers via help desk social engineering:** Organizations reported attackers using AI-generated voices to impersonate employees, successfully resetting credentials and bypassing MFA through processes outside IAM technical controls. (Source)
- **Hundreds of companies unwittingly hired North Korean operatives** using deepfake-enhanced video interviews, granting system access and privileged credentials because hiring verification relied on visual confirmation. (Source)
- **Stolen credentials were the most common initial access vector** according to the Verizon 2025 DBIR — used in 22% of breaches — increasingly obtained via deepfake-powered social engineering. (Source)

Bottom Line

Deepfakes expose the gap between what IAM systems verify (credentials, tokens, certificates) and what organizations need to verify (actual human identity during live interactions). Identity governance must extend beyond access control into identity assurance across all verification workflows.

Recommendation

Treat deepfake-enabled identity impersonation as a strategic IAM risk requiring cross-functional governance, enhanced identity proofing, and investment in phishing-resistant, deepfake-resistant authentication methods. IAM programs that focus solely on credential management will continue to experience identity failures in human workflows.

About GetReal Security

GetReal Security is the cybersecurity leader specializing in the detection and mitigation of threats posed by malicious generative AI content including deepfakes and impersonation attacks. Its technology serves multinational corporations, financial institutions, media organizations, government agencies, and social media companies.

The company was incubated by Ballistic Ventures, the venture capital firm dedicated exclusively to funding and incubating entrepreneurs and innovations in cybersecurity, and Dr. Hany Farid, the preeminent expert in media forensics.

getrealsecurity.com