GetReal

Deepfakes and Imposter Candidates:

HR's New Challenges Protecting the Enterprise Front Door

> *HR controls what's becoming an enterprise's most exposed entry point: the hiring process.*

What CHROs and TA Leaders Need to Know Now

To be blunt, your workforce may already include people hired under fake identities. Imposter candidates and fabricated employees are actively targeting remote hiring workflows at scale, using AI-generated personas, synthetic identities, and real-time deepfake video and audio to misrepresent themselves during interviews and onboarding. These attacks exploit the fundamental assumption underpinning remote hiring: that the person on the screen is who they claim to be.

AI changed the rules by making fake personas — assembled with photos, resumes, video presence, and spoken responses — dramatically more convincing and easier to iterate at scale. Remote work eliminated the natural verification that comes with in-person interaction, and deepfake technology has filled that gap with synthetic authenticity that passes traditional screening.

Remote hiring and AI-driven impersonation have converged into an operational threat that is already occurring at enterprise scale.

Why This Is a CHRO-Level Issue

You control the hiring gateway. You decide who becomes an employee, who gets onboarded, and who gains insider status — all before security controls activate.

This makes HR and talent acquisition the first and most critical line of defense:

- **Hiring integrity and workforce risk:** A single impostor hire can become an insider threat, plant ransomware, exfiltrate intellectual property, or compromise systems with privileged access
- **Operational and financial waste:** Time, budget, and effort spent sourcing, interviewing, onboarding, and compensating fraudulent employees represent direct losses
- **Remediation costs:** Discovering an impostor triggers legal review, security forensics, system audits, and potential regulatory reporting—all operationally disruptive and expensive
- **Employer brand and trust:** Public disclosure of impostor hires damages recruiting effectiveness and employee confidence in organizational judgment
- **Regulatory and compliance exposure:** Unknowingly hiring individuals from sanctioned entities (*such as North Korea*) violates UN Security Council resolutions and U.S. sanctions law, exposing the organization to federal enforcement, penalties, and reputational damage— with HR verification processes under direct scrutiny.

When hiring workflows treat video interviews as identity verification and assume that a face and voice equate to authenticity, impostors gain access with minimal friction. The cost of this failure extends far beyond HR — but this new accountability is increasingly placed on this function.

What “Reasonable Preparedness” Looks Like

Leading HR organizations are strengthening identity verification within hiring and onboarding processes to address the reality of AI-enabled impersonation:

- **Enhanced identity verification protocols:** Implement continuous identity verification that goes beyond video interviews and even onboarding to include biometric checks
- **Interview process hardening:** Train recruiters and hiring managers to recognize red flags (inconsistent video quality, reluctance to adjust camera settings, scripted responses, time zone discrepancies)
- **Vendor and recruiter pipeline controls:** Require third-party recruiters to implement identity verification standards and maintain audit trails for candidate sourcing
- **Cross-function collaboration:** Coordinate with IT and Security to monitor onboarding anomalies, unusual access requests, or behavioral inconsistencies post-hire
- **Background check enhancement:** Expand verification to include employment history validation through direct contact (not candidate-provided references) and multi-channel identity confirmation
- **Employee awareness and reporting:** Establish clear channels for employees to report suspicious new hires or unusual behavior from recent additions to the team

Real Consequences

This is not an emerging threat. Impostor hiring is happening now, at scale, with documented financial and operational impact:

- In July 2024, cybersecurity firm KnowBe4 discovered it had unknowingly hired a North Korean operative as a remote software engineer. The individual passed multiple video interviews and background checks, only to be caught days into employment when corporate sensors detected malware installation on company-issued equipment.
- CrowdStrike's 2025 Threat Report documented a 220% increase in companies that hired North Korean IT workers over a 12-month period, with more than 320 organizations infiltrated. Attackers used AI to forge identities, alter photos, guide interview responses, and mask their appearance in video calls.
- Reporting throughout 2024 showed companies hiring "employees" who later disappeared, were found working multiple jobs simultaneously under fabricated identities, or were discovered to have provided entirely synthetic credentials that passed initial screening.
- HR departments are increasingly targeted with impersonated internal requests to release employee data or modify records, using AI-generated voice and messaging that convincingly mimics leadership.

Bottom Line

Remote hiring now faces a threat that traditional screening can't catch: candidates who aren't real people. Impostors have already been hired at major companies — and executives and boards are looking to HR to answer for verification failures in systems they've designed and approved.

Recommendation

Treat identity verification as a critical control in hiring and onboarding, not an assumed outcome of video interviews. Establish continuous verification procedures that ensure biometric consistency in candidates across all interviews and onboarding. Require evidence beyond what candidates present on screen, and coordinate with Security and IT to detect post-hire anomalies.

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